International Journal of Information Management 32 (2012) 50–65

Contents lists available at ScienceDirect

International Journal of Information Management

journal homepage: www.elsevier.com/locate/ijinfomgt

Knowledge-Based Risk Management framework for Information Technology project

Samer Alhawari[a], Louay Karadsheh[b], Amine Nehari Talet[c,*], Ebrahim Mansour[a]

[a] Applied Science Private University, Jordan
[b] ECPI University, Raleigh, NC, USA
[c] King Fahd University of Petroleum & Minerals, Saudi Arabia

ARTICLE INFO

Article history:
Available online 30 August 2011

Keywords:
Risk
Risk management knowledge
Knowledge management
Knowledge-Based Risk Management
Risk response planning

ABSTRACT

The purpose of this paper is to explore the field of Risk Management (RM) in relation with Knowledge Management (KM). It attempts to present a conceptual framework, called Knowledge-Based Risk Management (KBRM) that employs KM processes to improve its effectiveness and increase the probability of success in innovative Information Technology (IT) projects. It addresses initiatives towards employing KM processes in RM processes by reviewing, interpreting the related and relevant literature and sheds light on integration with RM in the IT project.

The paper exposes some pertinent elements needed for building the KBRM framework for IT projects and also suggests some instrument about the integration of KM and RM process to improve the RRP (Risk Response Planning) process efficiency.

This paper will contribute to the literature and practice by providing a clear method for employing KBRM as a framework to keep organizations competitive within the business environment.

© 2011 Elsevier Ltd. All rights reserved.

1. Introduction

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. Holsapple and Joshi (2002) noted that a number of business and academic gurus that in order for organizations to have a lasting competitive advantage they will have to be knowledge driven. 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 (Karadsheh, Alhawari, El-Bathy, & Hadi, 2008). 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.

The world witnessed major turbulence in the global economy. These environmental changes may introduce new risks and organizations must arm themselves with comprehensive knowledge to address the risks introduced by this unstable environment promptly (Karadsheh et al., 2008). Many companies restructured themselves, some merged with others, filed for bankruptcy, acquired another company, and some implemented drastic layoffs. This resulted in a decrease in the resources available to all departments and a subsequent increase in business risks. Additionally, the U.S. economy has shrunk sharply since last autumn, with a real gross domestic product (GDP) having dropped at an annual rate of more than 6 percent in the fourth quarter of 2008 and the first quarter of 2009. One of the enormous costs of this economic downturn is the loss of 6 million payroll jobs over the past 15 months (Bernanke, 2009).

Another issue facing companies is globalization. The globalization of companies introduces many challenges. To meet these challenges, companies are required to become more innovative and introduce new ideas. The need to change is forcing corporations to organize their projects and their systems. Many companies depend on their own resources or external resources to meet their objectives and be better prepared for changes in their surrounding environment (Karadsheh et al., 2008).

Companies often utilize IT to develop innovative solutions in the hopes of having a competitive advantage. Additionally, Holsapple (2005) considers that knowledge management cannot be separated from computer-based technology. The IT systems attempt to streamline the business and reduce costs. IT enables businesses to integrate the operational, transactional, and financial information

* Corresponding author. Tel.: +966 506824421; fax: +966 38603489.
E-mail addresses: Samer.alhawari@yahoo.com (S. Alhawari), Louay.karadsheh@gmail.com (L. Karadsheh), nehari@kfupm.edu.sa (A. Nehari Talet), Ibraheem.m@asu.edu.jo (E. Mansour).

0268-4012/$ – see front matter © 2011 Elsevier Ltd. All rights reserved.
doi:10.1016/j.ijinfomgt.2011.07.002

processing. This information processing and reporting allows management to identify business risks and resolve risk-related issues (Karadsheh et al., 2008).

IT Projects are faced with many challenges and risks and new projects are conducted with fewer resources available. For example, the Standish Group's 2004 "CHAOS" study updated and incorporated data from several thousand software development projects, reveals that only 28 percent of an IT (Information Technology) projects were completed on time and on budget, down from a previous high of 34 percent. Another 18 percent (up from 15%) was canceled before completion of the development cycle, and the remained 51 percent were completed over-budget, behind schedule, and contained fewer functions than originally specified. Remarkably, CHAOS Summary 2009 results showed a marked decrease in project success rates, with 32% of all projects succeeding, which are delivered on time, on budget, with required features and functions. A comparison between the two reports portrays a continuous decline in IT project success.

In another study by "A Long Road Ahead for Portfolio Construction: Practitioners" (2009), a survey revealed that investment managers lack sufficient knowledge to manage risk optimally. This survey revealed more than half of the responded industry professionals saw the level of knowledge within their profession as the main barrier. Based on the authors "previous research in KM and practical experience in business, the author(s) realized the importance of KM in every aspect of private life and business. Furthermore, risks surround us in our personal and professional lives, and it is a potential problem that might happen. Moreover, most tasks require more and complicated steps, processes or procedures to accomplish. Therefore, to execute a task or process successfully, it seems essential to have the appropriate and the right knowledge that allow us to make the right decisions and responses called for during the execution. In this research, it is argued that knowledge is indeed needed and must be integrated carefully with RM to ensure correct execution. To obtain the integration of KM with the RM processes, the relationship between knowledge and risk has been examined to produce an integrated framework.

In a research conducted by Sallmann (2007), the existing RM services do not take advantage of KM. Introduction of KM concepts would provide better help against the changing risk environment. One way corporate risk managers in Industrial Corporation could improve their capabilities and services by applying a new knowledge-based approach. Furthermore, Massingham (2010) noted that there has been increased attention in application of knowledge management (KM) in managerial issues as a way of demonstrating the field's value. There has also been an increasing focus on risk management (RM) in reply to growing organizational awareness of corporate and social responsibilities.

Rodriguez and Edwards (2008) indicate that effective RM process modeling cannot be achieved without the assistant of a well-established KM process model. Therefore, a well-defined, designed and integrated KM and RM framework is essential to improve decision-making in IT projects (Rodriguez and Edwards, 2008). The goal of RM is to be more efficient in order to get better solutions for risk issues and to extend the experience, results, and solutions to more problems. RM also promotes the use of technology in an improved manner by having the organization use an integral risk information system

Based on a study by Shaw (2005), KM as a discipline can add positively to RM implementation in reference to data and information management, risk-knowledge sharing, analysis consolidation and reporting. Furthermore, RM is a discipline which organizations can no longer afford to ignore. Also, if companies are serious about both mitigating the effects of the threats, their operations encounter and seizing the opportunities that are passed their way, KM in turn must sit right at the heart of their RM strategy (Scott, 2002).

2. Literature review

2.1. Risk and Risk Management

Risks in an organization can span the gamut of natural disasters, security breaches, failings of human resource, third-part vendors, financial turmoil, unstable business environments and project failures. 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) (Project Management Institute, 2004). 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 (Project Management Institute, 2004). Furthermore, risk refers to all events, occurrences and actions that may prevent you or your organization from realizing its ambitions, plans and goals. Risk surrounds us in our personal and professional lives and is a potential problem that might happen. Regardless of the outcome, it is a good idea to identify risk, assess its probability of occurrence and estimate its impact. The reasons for studying RM vary, for instance, some people study it to prepare for a career in a specific field and others study it as a part of a general business curriculum (Alryalat & Alhawari, 2008).

Padayachee (2002) describes risk as any variable in the project that causes project failure. However, there is a common agreement between researchers, that risk has a probability attribute which is called in some definitions "likelihood", "probability of occurrence" and "frequency of occurrence". A second attribute typically related to a risk is what is called the "impact", "severity", "consequence" (Carbone & Tippett, 2004). In general, risk can have two-dimensional meaning, namely negative and positive events (Olsson, 2008). Jaafari (2001) defines risk as the probability of loss or gain occurrence multiplied by its respective magnitude. A Guide to the Project Management Body of Knowledge-PMBOK (2004) defines risk as an uncertain event that has a positive or negative impact on the project's objectives. Other researchers argue that risk is mostly related to project barriers and threats. For example, Miles and Wilson (1998) define risk as a barrier to success.

Risk Management has developed rapidly over the recent decades as an integral part of project management (Del Cano & Cruz, 2002). It includes the processes concerned with RM planning, identification, analysis, responses, and monitoring and control on a project "(PMBOK, 2004).

RM is a distinct discipline, which integrates knowledge from a variety of other business fields. It is the discipline where wide varieties 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 (Del Cano & Cruz, 2002). RM refers to strategies, methods and supporting tools to identify, and control risk to an acceptable level (Bruckner et al., 2001). RM is a distinct discipline, which integrates knowledge and methodologies from a variety of other business fields to bear on a specific problem. The RM objective is to identify all applicable risks in a project, 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 (Cule, Schmidt, Lyyttnen, & Keil, 2000). 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 pursing their goals.

Roy (2004) points out that software development projects are particularly demanding for risk analysis. They include a wide variety of risk factors across a number of different stakeholder's predetermined perspectives. RM for software projects is intended to minimize the chances of unanticipated events, or more purposely to keep all possible outcomes under firm management control (Roy, 2004). Moreover, RM must be an integrated part of the project management framework if it is to be effective. Furthermore, RM is concerned with making judgments about how risk events are to be treated, valued, compared and combined (Roy, 2004). The propose of RM is to develop a detailed analysis of the organization and project domains to develop a complete set of risk factors and to ensure they are appropriately organized to reflect all the stakeholders and the various risk perspectives that are required (Roy, 2004).

Tesch, Kloppenborg, and Frolick (2007) indicate that the failure of IT systems development projects has been well documented. While there are many reasons for these failures, they can typically be categorized as cost, time and performance or quality issues. Tesch et al. (2007) identify a list of 92 risk factors that were presented to members of the PMI for ranking. The result of the ranking was the categorization of systems development risk factors as well as the judgment of their perceived importance of each specific risk within each category. The purpose of the research's Tesch et al. (2007) is to better understand IT project risk factors from a Project Management Professionals (PMP) perspective. Furthermore, to develop how to use the strategies both by creating a project management system with well-defined roles and by describing how to use the strategies at certain key points during a project's life. The result is a Project Risk Management approach involves the systematic process of identifying, analyzing and responding to project risk. According to Tesch et al. (2007) project risk involves understanding the probability for problems as they might hinder project success. Finally, the RM project's objectives are to minimize the probability and impact of potential risks while maximizing the probability and impact of potential opportunities.

2.2. Knowledge and Knowledge Management

In order to have a new knowledge economy and business, organizations are now facing major challenges due to external pressures as well as the nature of the workplace. This provides rises to the necessity of improvement of a strategic, comprehensive, holistic and adoption Knowledge Management (KM) to enhance the process and get the competitive advantage (Nehari-Talet, Alhawari, & Alryalat, 2010). As a result, KM has begun to be proactively introduced within the policy, strategy, and implementation processes of worldwide corporations, governments, and institutions (Malhotra, 2005). Davenport and Prusak (1998) describe knowledge as a mix of framed experience, values, contextual information and expert insight that provides a structure for evaluating and integrating new experiences and information. It originates and is applied in the minds of the knowledge workers. In organizations, it often becomes embedded not only in documents or repositories, but also in organizational routines, processes, practices and standards (Davenport & Prusak, 1998).

Holsapple and Joshi (2004) define that KM as an entity's systematic and deliberate efforts to expand, cultivate, and apply available knowledge in ways that add value to the entity, in the sense of positive outcome in achievement its objectives or fulfilling its purpose.

Knowledge can be viewed as the result of merging information with practice, perspective and expression, resulting in insinuation and presents approaches and plans on which decision is based on (Kahn & Adams, 2000). Also, Michael, Zhdanova, and Fensel (2004) define knowledge as information used for resolving a precise dilemma, which presents the realistic stage. Moreover, Alavi and Leidner (1999) describe KM as an organized and systemic process for acquiring, organizing and exchanging knowledge among employees to effectively utilize knowledge.

KM is an art of transforming information and intellectual assets to a permanent value for the organization, its partners and clients (Marin-Garcia & Zarate Martínez, 2007). KM is defined by Alryalat and Alhawari (2008) as a procedure, process, or practice to accomplish the process about knowledge, process for knowledge and process from knowledge, which leads to an improvement in the internal and external operation. Moreover, Kim, Lim, and Mitchell (2004) define KM as the methodical means of administrating this valuable resource, by promoting an incorporated approach to identifying, capturing, structuring, organizing, retrieving, sharing, and evaluating an enterprise's knowledge assets. Furthermore, Miltiadis, Pouloudi, and Poulymenakou (2002) built a new mechanism for exchanging and generating new knowledge mechanism. Kim et al. (2004) define KM as the methodical means of administrating this valuable resource, by promoting an incorporated approach to identifying, capturing, structuring, organizing, retrieving, sharing, and evaluating an enterprise's knowledge assets. Also, Goh (2005) describes KM as a methodical leveraging of data, information, proficiency and different structures of assets and resources to enhance organizational innovation, reaction, efficiency and capability. It represents the significant issues of organizational procedures, through the exercise of suitable technologies to connect dissimilar kinds of knowledge assets.

2.3. The Role of Knowledge Management Process in Project Risk Management

KM and its Risk require significant attention within the majority of twenty-first century organizations. Additionally, Massingham (2010) noted that Knowledge risk management (KRM) is an emerging field which suggests a solution to the problems connected with conventional risk management methods. The problem of environmental complexity is manifested by individuals not knowing enough about the risk to anticipate its likelihood and consequences.

According to Neef (2005), 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. A project failure can be the result of capturing the appropriate knowledge at an inappropriate time of the project (Fuller, Valacich, & George, 2008). In fact, without KM as a tool to communicate risks among members of a project team, RM might suffer from ineffectiveness and inefficiencies (Schwalbe, 2007).

Owen (2006) develops a KM framework 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. 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 (Fuller et al., 2008). 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.

Neef (2005) has found that 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. 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.

Jones (2005) analyzed how 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. This pilot audit has improved the understanding and application of information and KM in the Council. 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 by Caldwell (2008), three core KM principles related to RM have been noted. 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, Caldwell (2008) stated that KM accountability requires domain experts to be assigned to work with knowledge managers to maintain various information sources.

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 (Perera & Holsomback, 2005). Our proposed KBRM framework for IT project was designed based on a thorough investigation of various models presented by different authors. The authors introduced a new methodology that contributes in providing guidance for developing risk modeling knowledge in order to improve the quality and quantity of RM processes. As shown in Fig. 1, the authors 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.

As a result, their proposed methodology used the context and experience to improve the risk modeling process and its 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 is described in Tah and Carr (2001). The paper 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.

Kayis et al. (2007) develop a comprehensive RM tool called IRMAS (Intelligent Risk Mapping and Assessment System). This RM tool contains some KM tools and techniques. The first process is Context Establishment, which defines organizational, and user details, project objective, ownership, management support, regulatory requirements, nature of the project, type of project, schedule cut-off dates, estimated project budget, mitigation budget and government and/or regulatory authorities that needed to be complied. The purpose is to establish overall risk profile by assigning a weighting to the infrastructure of the organization after the user's responses to a series of questions, covering the above-mentioned issues. The answers will be captured based on questions retrieved from the Expert Interview Facility (EIF); a database where all phase questions are stored and displayed to the users via the virtual workbench. The virtual workbench is to promote interactions with other project participants and facilitate communication. Fig. 2 describes IRMAS.

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.

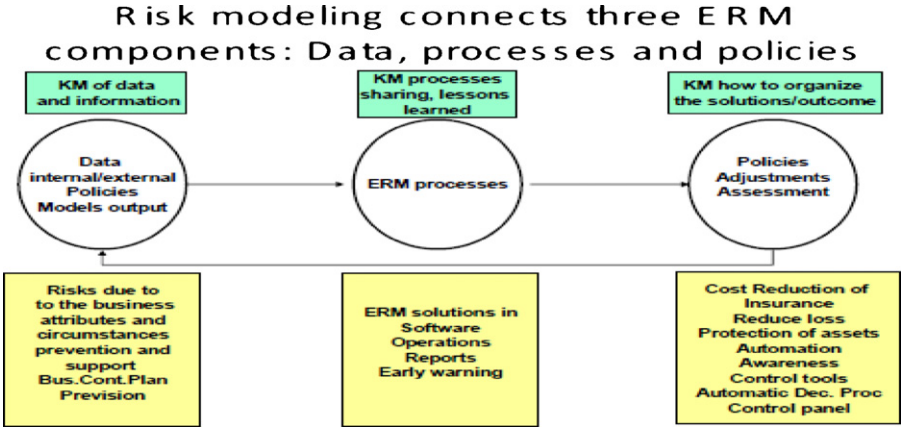


Fig. 1. Knowledge Management Acts through Risk Modeling in Different Components of Enterprise Risk Management Processes in Rodriguez and Edwards (2008).

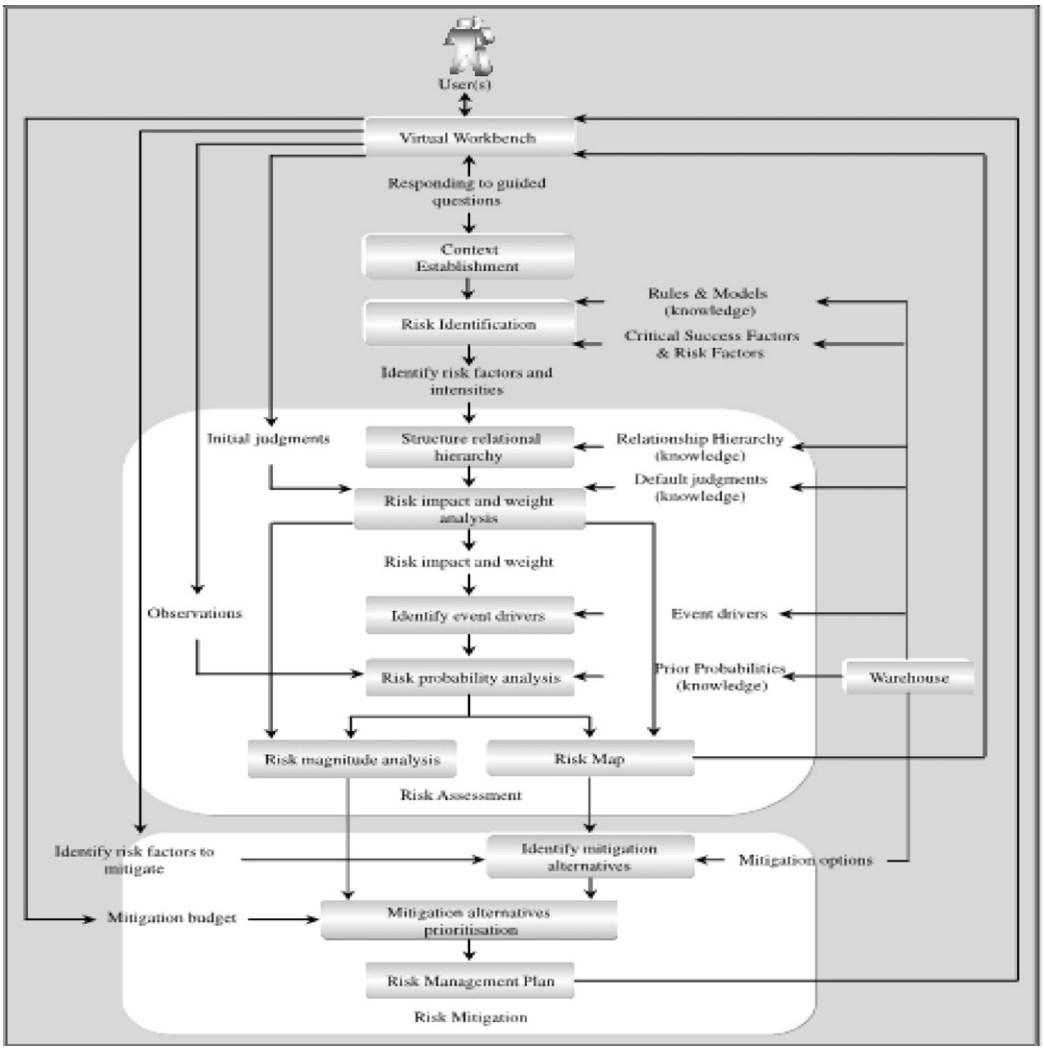


Fig. 2. Intelligent Risk Mapping and Assessment System.

Finally, the aim of this research project is to propose a conceptual framework of the KBRM processes, that addresses KBRC (Knowledge-Based Risk Capture), KBRD (Knowledge-Based Risk Discovery), KBREx (Knowledge-Based Risk Examination), KBRS (Knowledge-Based Risk Sharing), KBRE (Knowledge-Based Risk Evaluation), KBRR (Knowledge-Based Risk Repository) and KBREdu (Knowledge-Based Risk Education) The expectation is that this research will contribute to the body of knowledge related to RRP in IT projects (Karadsheh et al., 2008).

3. The proposed Knowledge-Based Risk Management framework for Information Technology projects (RiskManIT)

The proposed Knowledge-Based Risk Management framework (RiskManIT) illustrates the role of KM processes in enhancing and facilitating risk identification, analysis, risk response planning and execution processes. The purpose is to develop a road map for the organization to implement this conceptual framework for any IT project. Moreover, the application of KM to RM requires on one hand, the identification and development of knowledge processes, and on the other hand, the identification of the integral knowledge that a knowledge worker requires in particular the risk modeling knowledge (Rodriguez & Edwards, 2008).

The framework is divided into two sections. Section one is the RM process and section two is the integration of KM and RM in the proposed framework.

3.1. Risk Management Process in the proposed framework

Since the framework objective is to improve RM processes by adding KM elements, therefore, this section discusses the main component of RM processes first. It starts with Scope Establishment, Risk Identification, Risk Analysis, Risk Response Planning, Risk Education and finally, Risk Monitoring.

3.1.1. Scope establishment

Knowledge-Based Risk Capture supports the first process of RM, which is scope establishment. According to Mees (2007), scope establishment process describes the targeted information system, its boundaries, environment, identity and its stakeholders' objectives. Moreover, Stonebumer, Goguen, and Feringa (2002) state that system characterization is required to define the IT project scope by identifying the system boundaries, along with the resources and the information that constitutes the system. System characterizing means establishing the scope of the risk assessment effort, delineating the operational authorization boundaries, and providing information (e.g., hardware, software, system connectivity, and

responsible division or support personnel) essential to define the risk.

During this stage, stakeholders' requirements are captured to help in making informed decision involving risks. Also, RM policies describe the guidelines under which RM is explicitly defined should be established along with a description of the procedures to be followed in the RM process. Roles, responsibilities, and the needed resources for performing RM processes should be assigned. Finally, a description of the evaluating process that will be followed should be created. Any relevant lessons from a prior use of the process should be incorporated into the implementation of the process ("Systems and software engineering – Life cycle processes – Risk management," 2006).

The output of this process is a complete IT project profile with information regarding the IT project in hand. The purpose is to provide information on what is the purpose, information system, resources needed and requirements.

3.1.2. Risk Identification

Risk identification process determines which possible risks might affect the project and documents their characteristics (PMBOK, 2004). Sources of risk and potential consequences need to be identified, before they can be acted upon to mitigate (Kayis et al., 2007). Therefore, KBRC process captures all risks from previous reports, lessons learned, other similar incidents and relevant articles as explicit knowledge. In terms of tacit knowledge, this process plays a major role in capturing the risks from people based on their experiences, which relied on their problem solving expertises. The result of the capturing process is stored in the explicit form which contains a list of all the identified risks, and it should be made accessible to involved personnel. Also, during this stage the historical and current RM circumstance and risk state information are captured. This helps in creating a project risk profile which contains a total of all the individual risk profiles and risk states ("Systems and software engineering – Life cycle processes – Risk management," 2006).

Various approaches can be used for risk identification. These approaches may include the use of risk questionnaires, taxonomies, brainstorming, scenario analysis, lessons learned, and prototyping or other knowledge capturing approaches. Repeatable identification processes may be used to assist in the capture of lessons learned. Where possible, events, hazards, threats, or situations that can create risks should be identified to aid future risk treatment ("Systems and software engineering – Life cycle processes – Risk management," 2006). The output of the risk identification process is a full documentation that describes IT project assessed, the environment surrounding IT project, and the project objectives. This result is an IT risk project profile.

Also, in risk identification process, knowledge discovery assists in discovering new risks associated with the company or a particular project. Managing risks appropriately, requires identifying the source of each risk, which might include a variety of causes such as technology content, surroundings interaction, constraints and operation and execution approaches (Cornford, 1998).

3.1.3. Risk analysis

Risk analysis facilities the conversion of risk data into decision making information (Higuera & Haimes, 1996). Each risk identified in the previous stage will be analyzed in this process. Team members will share their experience about the identified 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 (Alhawari, Thabath, Karadsheh, & Hadi, 2008). According to ("Systems and software engineering – Life cycle processes – Risk management," 2006) 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 (Alhawari et al., 2008). Also, risk analysis will categorize the risks based on the likelihood of occurrence, impact and extend of loss (Higuera & Haimes, 1996). The output of the risk analysis process is a detailed description of every valid risk, severity, impact, priority, probability and impact estimates. This process provides the means to establish the needed security controls in order to reduce the impact of the risk to an acceptable level by the organization (Alhawari et al., 2008).

3.1.4. Risk response planning

RRP (risk response planning) assists in converting the risk information into actions and judgments. RRP involves developing actions to deal with each risk, prioritizing measures, and creating a management plan (Higuera & Haimes, 1996). This process takes the collected information to formulate plans, strategies and actions, and its ultimate goal is to reduce both the probability of risk occurrence and the degree of that loss (Bruckner et al., 2001). The RRP 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 likelihood of risks. This process also provides different execution possibilities and examines different "What-if" options. The goals of this process are: (1) Reduction of the probability of risk occurrence; (2) reduction of loss magnitude; or (3) changing on risk's consequences (Bruckner et al., 2001).

The planning process outputs according to Beck, Drennan, and Higgins (2002) are simple rules, process controls, testing, modeling and inheritance. Additionally, 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 has been 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 ("Systems and software engineering – Life cycle processes – Risk management," 2006) 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 (Farias, Travassos, & Rocha, 2003). Once stakeholders reach an agreement on which risk treatment is accepted. A detail treatment plan should be defined on how to be executed. Also, during this stage the reporting and communication is established to the stakeholders. The purpose is to share the knowledge obtained during the execution process ("A Risk Management Standard," 2002).

3.1.5. Risk execution

According to Mees (2007), risk can be treated in a number of ways: (1) *Risk avoidance*: means simply not performing the activity that carries the risk; (2) *Risk reduction*: involves approaches that reduce the probability of the vulnerability being triggered or reduce the impact when the vulnerability is triggered. Risk control is implemented; (3) *Risk transfer*: means passing the risk on to another party that is willing to accept the risk, typically by contract or by hedging. A good example is insurance; (4) *Risk retention*: means accepting the loss when it occurs. This is applicable to

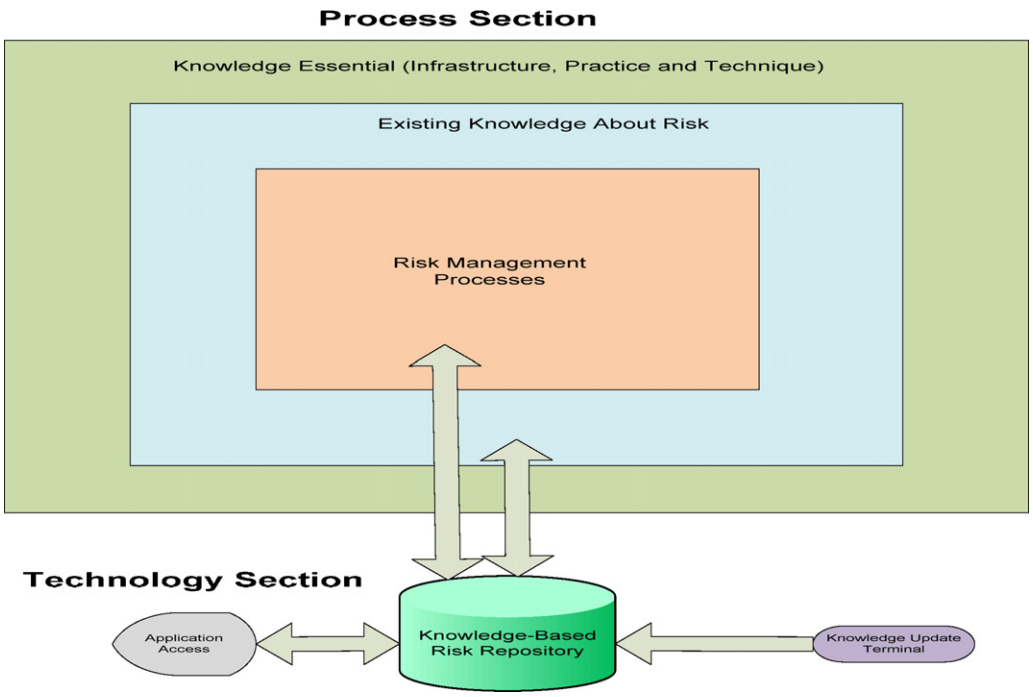


Fig. 3. Context diagram for the proposed Knowledge-Based Risk Integrated framework (Karadsheh et al., 2008).

low impact risks. During the execution process risk control 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 (Perera & Holsomback, 2005). This might require starting from risk identification, which in turn needs to communicate with KBRC for further analysis and examination.

3.1.6. Risk monitoring

In this process, risk monitoring is viewed as a feedback process. The purpose of risk monitoring is to: (1) Review and update the individual risk states and the RM context. (2) Assess the effectiveness of risk treatment. (3) Seek out new risks and sources ("Systems and software engineering – Life cycle processes – Risk management," 2006). Also, risk must be monitored to ensure that any control measures are working and to enable effective action to be taken if the risk occurred. The monitoring process continues to ensure that the assessment and handling procedures are effective and, if so, that the corrective actions and strategies are working. If any of these had been proven 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 IT project if their chance of occurrence has passed, or if they have been dealt with (Tah & Carr, 2001). Removing a risk from the project doesn't mean no documentation is preformed for future reference.

Project team members will meet to exchange their knowledge and evaluate the outcome. According to Systems and software engineering – Life cycle processes – Risk management Standard ("Systems and software engineering – Life cycle processes – Risk management," 2006) three steps are important to monitor risk performance: (1) Monitor risk throughout the project life cycle to detect any changes in its state using measures that will be recorded in the project risk profile. (2) Measures shall be implemented and monitored to evaluate the effectiveness of risk controls. (3) 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. According to Risk Management Standard ("A Risk Management Standard," 2002), 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 is been evaluated by the KBRE process occasionally typically every bi-week.

3.2. The integration of knowledge management and risk management in the proposed framework

Adding KM components to RM processes will produce the following processes: (Knowledge Essentials), KBRC (Knowledge-Based Risk Capture), KBRD (Knowledge-Based Risk Discovery), KBREx (Knowledge-Based Risk Examination), KBRS (Knowledge-Based Risk Sharing), KBRE (Knowledge-Based Risk Evaluation), KBRR (Knowledge-Based Risk Repository) and KBREdu (Knowledge-Based Risk Education). This illustration will be described thoroughly in this section.

The next paragraphs will be focused on finding the links between KM processes and RM processes by describing the relation in high level diagrams (Karadsheh et al., 2008). Fig. 3 illustrates a context diagram for the KBRM integration.

Fig. 3 contains two sections, the technology represented by the repository environment and the process section represented by KM and RM environment. It also portrays knowledge essentials as components that contain the foundation for utilizing knowledge and the practices and techniques options used to employ, capture and share knowledge throughout KM processes. Fig. 4 illustrates the interaction of employees with the proposed KBRM framework using Use Case tools.

Fig. 5 is a UML class diagram of the Meta model of the proposed KBRM framework. The purpose of the UML diagram is the modeling of the important components of the proposed KBRM framework and their relationships using a graphic notation, and is instantiated after adoption by a client.

Fig. 6 illustrates the new KBRM framework which contains (Knowledge Essentials), KBRC (Knowledge-Based Risk Capture), KBRD (Knowledge-Based Risk Discovery), KBREx (Knowledge-Based Risk Examination), KBRS (Knowledge-Based Risk Sharing),

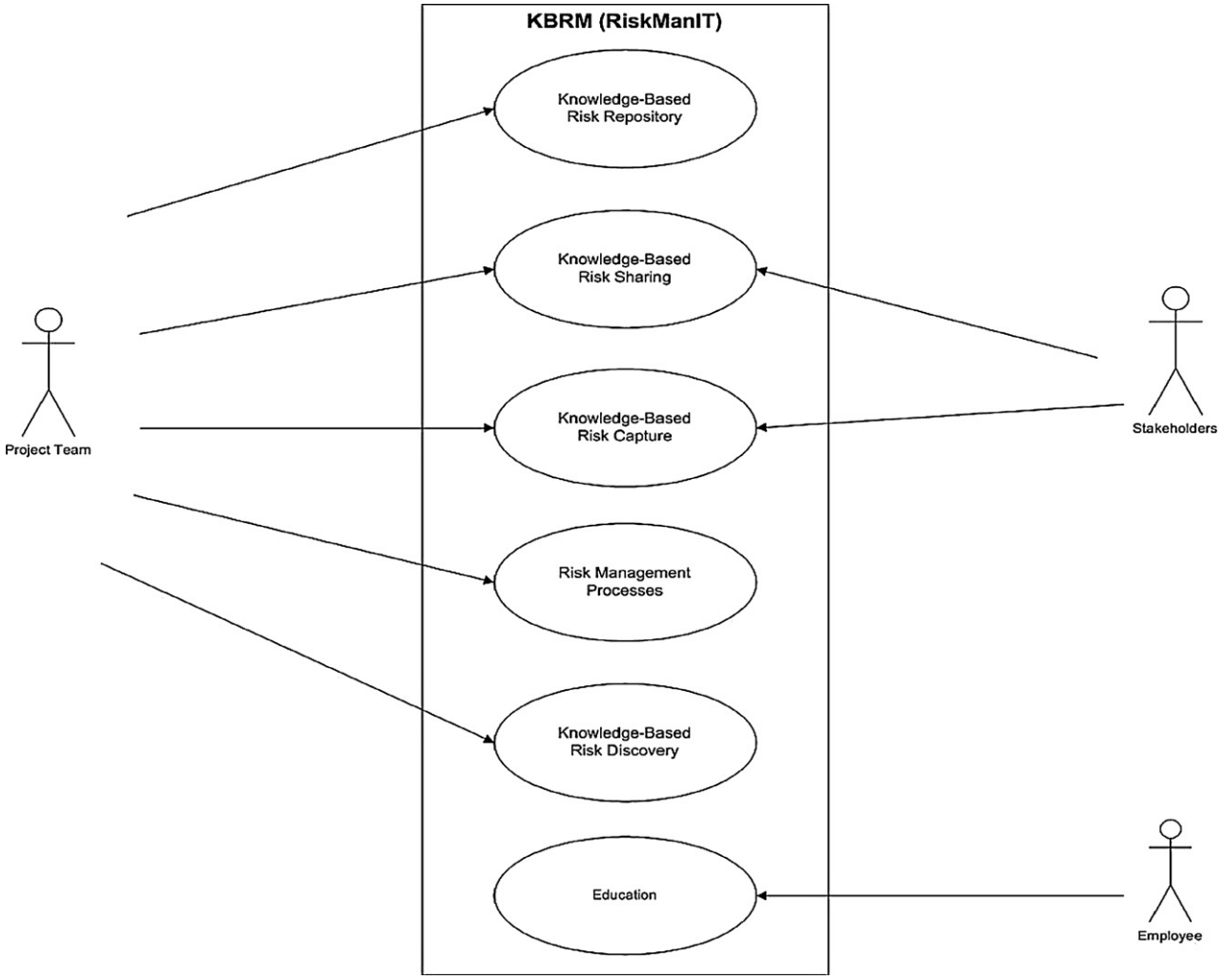


Fig. 4. Use case context diagram for the proposed KBRM framework (Karadsheh et al., 2008).

KBRE (Knowledge-Based Risk Evaluation), KBRR (Knowledge-Based Risk Repository) and KBREdu (Knowledge-Based Risk Education) are illustrated in relation to RM processes. These elements are fully discussed in this section.

3.2.1. Knowledge essentials

Knowledge essentials contain two important primary items, namely Knowledge Infrastructure and KM Practices and Techniques to support the KBRM framework.

Knowledge infrastructure represents social capital, the relationships between knowledge sources and users, and is operationalized by technology (the network itself), structure (the relationship), and culture (the context in which the knowledge is created and used) (Jennex, 2005).

The technology can be document management systems and yellow pages used as KM systems to facilitate knowledge capturing and storage (Neef, 2005). Structure promotes collective rather than individual behavior, thus encouraging interpersonal interaction and sharing of knowledge among employees. Finally, culture is defined by Gold, Malhotra, and Segars (2001) as "shared and widely accepted values and visions that permeate in mind to direct work practice or facilitate necessary changes.", the purpose is to infuse knowledge vision to everyone visibly, regularly, and extensively (Chan & Chao, 2008).

Knowledge Management techniques that support risk modeling knowledge processes are associated with interdisciplinary work, interdepartmental work controlling the whole process from problem definition to solution evaluation. Some of these techniques are: communities of practice, forums, training, conferences, post project reviews, mentoring; yellow pages and so on (Rodriguez & Edwards, 2008).

Moreover, Neef (2005) lists some important KM techniques and systems used by organizations such as: knowledge mapping, communities of practice, hard-tagging experts, perform monitoring and reporting, community and stakeholder involvement, business research and analysis. Furthermore, Becerra-Fernandez, Gonzalez, and Sabherwal (2004) state additional KM techniques and tools used by organizations such as: data mining, stories telling techniques, best practice database, lessons learned and Expertise-locator (EL) system.

Therefore, knowledge infrastructure contains components that focus on building a base system to capture and distribute knowledge for use throughout the organization (Jennex, 2005). KM practices and techniques provide several options to be used by the organization to capture tacit and explicit knowledge and share it throughout the KM processes. This structure covers all processes and can be used as a base to execute any process.

3.2.2. Knowledge-Based Risk Capture

Knowledge-Based Risk Capture supports two important RM processes: scope establishment and risk identification. In this section,

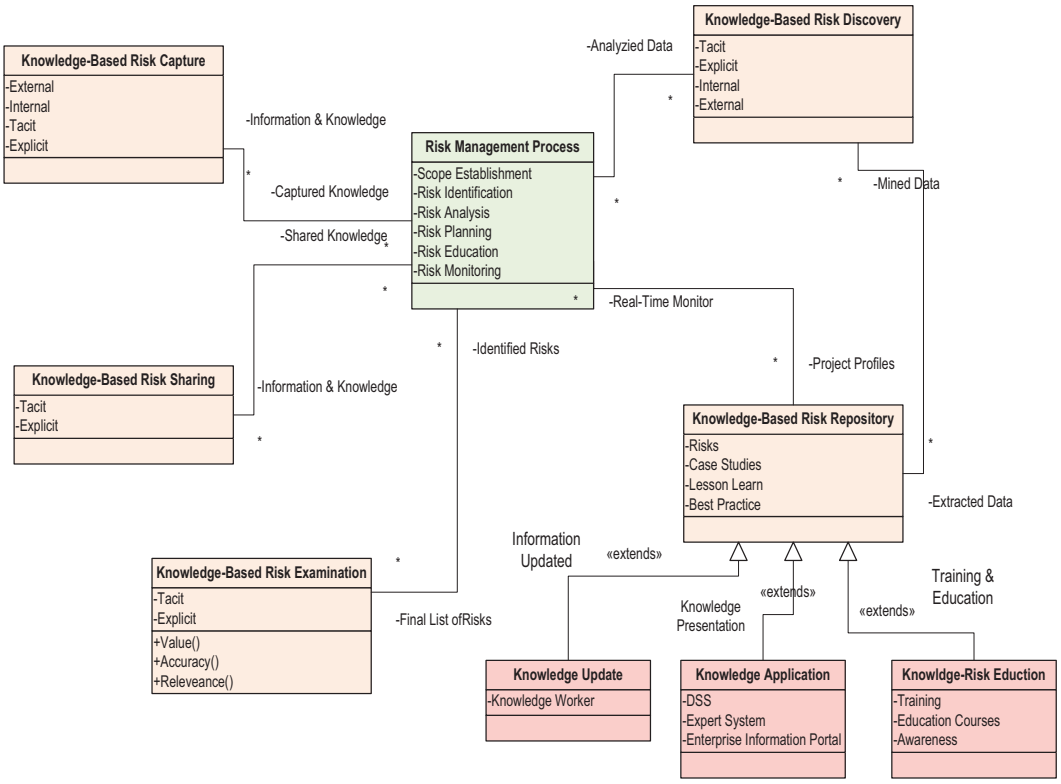


Fig. 5. Meta-model for the proposed KBRM framework (Karadsheh et al., 2008).

a description KBRC purpose, followed by its support to scope establishment and risk identification.

In this conceptual framework, the first element is the KBRC process. KBRC focuses on capturing both the explicit and tacit knowledge exist within people and artifacts inside and outside the organization (Becerra-Fernandez et al., 2004). Its main components are: externalization and internalization. Externalization involves converting tacit knowledge into explicit knowledge through several mechanisms such as: models, prototypes, best practices and lessons learned (Becerra-Fernandez et al., 2004). Using various mechanisms such as: learning by doing, on-the-job training, learning-by-observation and face-to-face meetings (Becerra-Fernandez et al., 2004). Moreover, McElroy (2000) claims that any process that involve intentionally capturing knowledge or information formed by external users to the organization as an Information acquisition process. Another definition by Holsapple and Joshi (2002) stated that knowledge acquiring is defined as an activity that accept any knowledge from the external environment and transforming it into a representation that can be internalized, and/or used within an organization. This involves extracting knowledge from external sources, interpreting the extracted knowledge and transferring the knowledge (Holsapple & Joshi, 2002).

Fig. 7 illustrates the activities, input and output associated with KBRC process.

3.2.3. Knowledge-Based Risk Discovery

Knowledge-Based Risk Discovery supports two important RM processes: scope establishment and risk identification. Knowledge discovery is defined as the development of a new tacit or explicit knowledge from data and information or from the fusion of prior knowledge (Becerra-Fernandez et al., 2004). KBRD starts by discovering organizational knowledge related to IT projects or any other type of project by sharing of tacit knowledge, so that individual unexplored knowledge can be amplified inside the organization. Next, the shared tacit knowledge is converted into explicit knowledge to form a new concept. At this point, the organization must determine if the new concept is sufficiently relevant to be validated in order to justify it. All of the new concepts are converted into a template, where the created knowledge is extended to other organization teams, or even to external elements (de Rezende & de Souza, 2007). Moreover, KBRD process in the organization requires discovering new risks or replacing the existing risks that do not apply to the organization in the current time based on the organization's tacit and explicit knowledge (Pentland, 1996). Fig. 8 illustrates the activities, input and output associated with KBRD process.

Utilizing data mining techniques in KBRD can aid in uncovering new relationships between explicit data that may lead to categorization models that create new knowledge (Becerra-Fernandez et al., 2004). Therefore, data mining or knowledge discovery is the process of analyzing data from different perspectives and summarizing it into useful information (Qi, 2008) that can be used to identify risks related to a specific an IT project. Knowledge discovery interacts with the knowledge repository and utilizes data mining techniques to discover trends in the data that were not known previously (Becerra-Fernandez et al., 2004). For example: given the profile of a new project, it is possible to collect information about any other project that has similarities with the current one, be aware of people that are interested in the same subject, or identify documents that talk about the same argument (Agostini, Albolino, Michelis, Paoli, & Dondi, 2003).

Moreover, KBRD can perform pattern discovery on previous an IT projects with the new one. According to Senator (2005) supporting this pattern matching task is the task of discovering patterns. While pattern matching may be thought of as inference, pattern discovery is more properly thought of as learning. Therefore, KBRD helps in identifying risks more efficiently and effectively through utilizing data mining techniques.

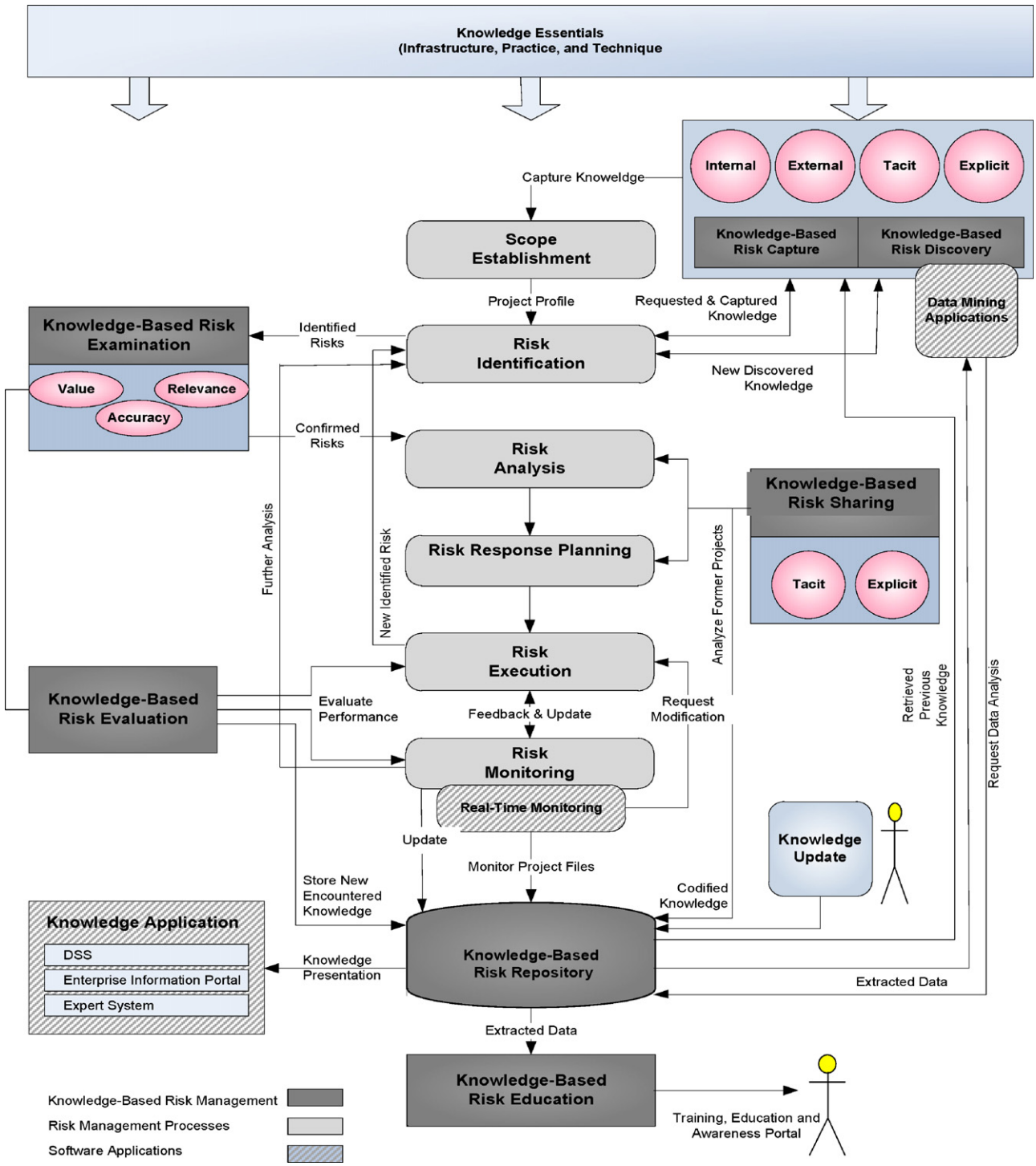


Fig. 6. A conceptual framework for Knowledge-Based Risk Management (Karadsheh et al., 2008).

3.2.4. *Knowledge-Based Risk Examination*

KBREx (Knowledge-Based Risk Examination) contains the knowledge examination process which focuses on examining risk content against accuracy and correctness (Karadsheh et al., 2008). This process aims to support the risk identification process and to produce the final relevant risks which are applicable to the organization. In addition, analyzing prospective risks through assigning a value to the impact of each risk on the project progress requires knowledge brainstorming and team discussion sessions (Cornford, 1998). Fig. 9 illustrates the activities, input and output associated with KBREx process.

Knowledge examination process is used to assess the knowledge based on the value, accuracy and relevance after combining the knowledge from different sources (Karadsheh, Mansour, AlHawari, Azar, & El-Bathy, 2009). Furthermore, McElroy (2000) stated that any knowledge claim by the organization should be subject to criteria to determine the value and veracity. The knowledge in this process refers to knowing risks or knowledge of risk. Knowledge can be assessed based on its relevance to the organization, management strategy and business strategy (Sunassee & Sewry, 2002). Therefore, knowledge examination helps to assess the identified risks based on its value, relevance and accuracy in reference to an

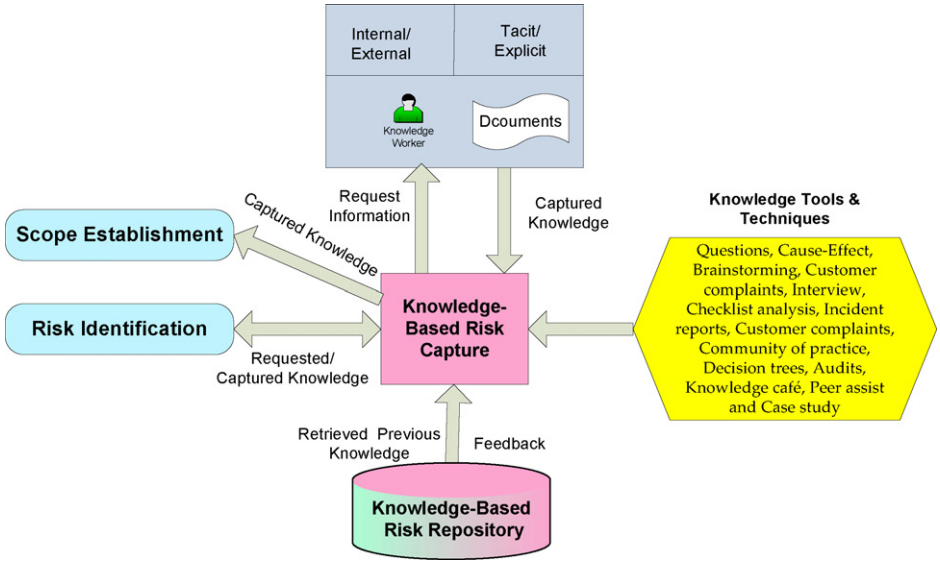


Fig. 7. Knowledge-Based Risk Capture process.

IT project. Once risks have been evaluated then it is ready for risk analysis process.

Finally, KBREx process eliminates risks that are not related to the project progress or company's objectives and goals (Karadsheh et al., 2008). Therefore, the final output will contain only confirmed risks for the specific an IT project.

3.2.5. *Knowledge-Based Risk Sharing*

KBRS (Knowledge-Based Risk Sharing) supports two important RM processes: risk analysis and risk response planning. In the beginning, a detailed description of KBRS and its impact on the two RM processes, followed by description of both risk analysis and risk response planning.

KBRS (Knowledge-Based Risk Sharing) is based on allocating knowledge among stakeholders to exchange their tacit knowledge about risks that are elected or produced exterior or within the organization and to document any newly identified risks. Knowledge sharing is executed by disseminating and exploiting the captured or discovered knowledge from the organization whether the source is internal or external (Sun & Gang, 2006).

KBRS (Knowledge-Based Risk Sharing) is viewed as iterative process for both, risk analysis and planning processes because during risk analysis, a new risk might expose and requires knowledge collaboration to assess its impact and severity. Also, KBRS supports knowledge transfer from individual to another individual in a collaboration environment. Therefore, the project team involve in evaluating the risks surrounding either the project execution can share their experiences in the progress, will serve as input to the risks analysis or the risk response planning for purpose of modifying the sub-processes of both. Through this process, the team should decide on the appropriate method for executing risk analysis and risk response planning. The tools used to facilitate knowledge sharing process are best practice database, alert system, lessons learned and expertise locator (Baccarini, Salm, & Love, 2004).

Moreover, Neef (2005) stresses on the importance of having knowledge-sharing culture, which is an organizational culture in which values and expectations for ethical behavior need to be communicated widely and effectively throughout the organization. Therefore, knowledge-sharing culture plays a key role in the KBRM framework. There are needs to have a regular and consistent communication on values and on processes that encourage shar-

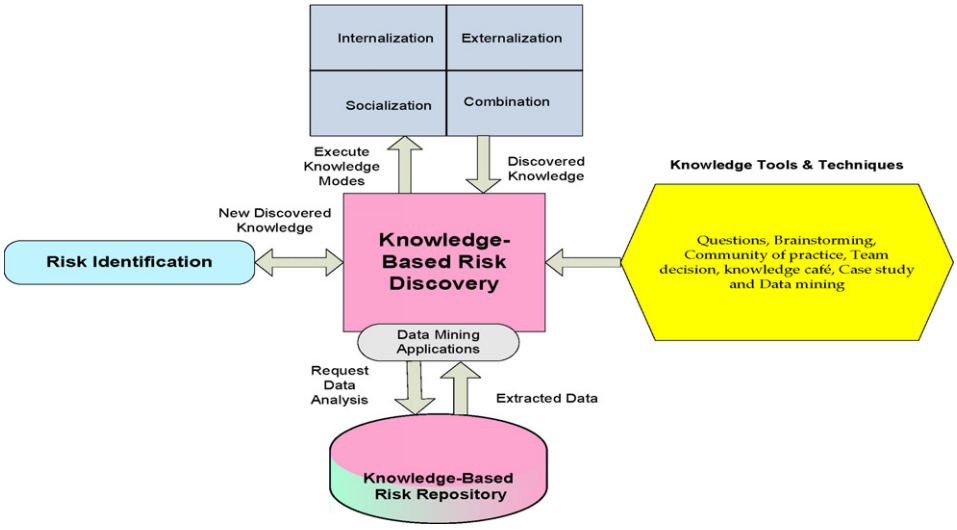


Fig. 8. Knowledge-Based Risk Discovery process.

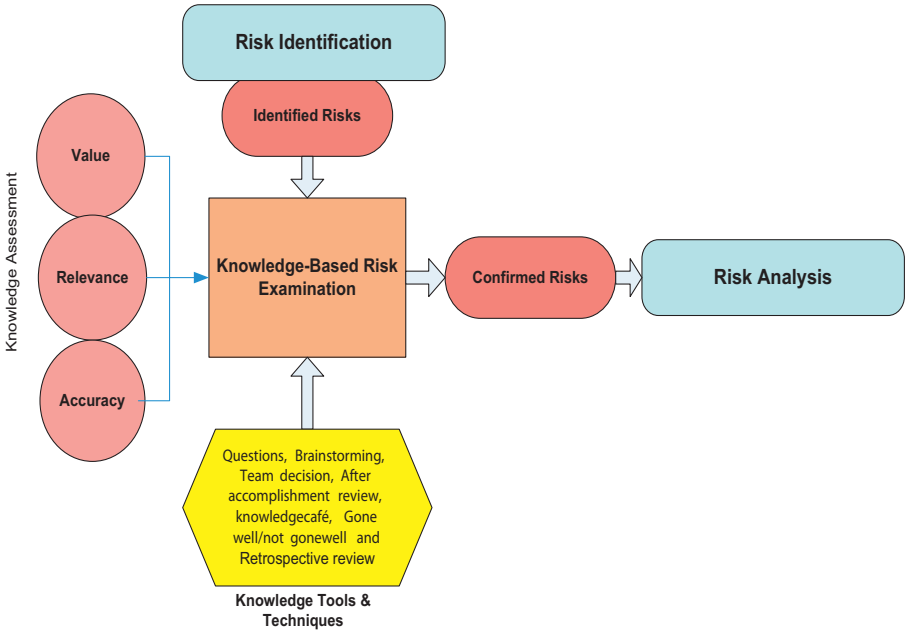


Fig. 9. Knowledge-Based Risk Examination process.

ing of ideas and early identification of risks. Fig. 10 illustrates the activities, input and output with KBRS process.

3.2.6. Knowledge-Based Risk Evaluation

KBRE (Knowledge-Based Risk Evaluation) process serves as an assessment process for the risk execution process in an on-going basis by tackling risks in weekly, monthly or quarterly basis (Kasap & Kaymak, 2007). Also, this process will evaluate the risk execution progress and risk control mechanisms continuously. Therefore, this process will function as a continuous process leading to either retiring an existing risk once a solution is attained or identifying a new risk (Fayda, Ulusoy, & Meyanli, 2003). Moreover, during the process, knowledge sharing of experience encountered throughout the execution of the risk project will assist in modifying the process to maintain accuracy. Moreover, capturing of information encountered during the risk execution should be stored in the KBRR. Fig. 11 illustrates the activities, input and output associated with KBRE process.

3.2.7. Knowledge-Based Risk Repository

The lack of documentation on the success or failure of past experiences is one of the reasons for inefficient RM utilization or non-utilization in software development organizations. Therefore, the past experience analysis is fundamental to help project managers in risks planning and controlling (Farias et al., 2003).

Tah and Carr (2001) suggest a KM system that will be developed to monitor risk, task, and project profiles. This will eventually provide decision support by suggesting risks and actions that may affect specific task types on new projects, based on previous project risk reports. KBRR process purpose is to integrate KM database and RM database as a single database to maintain up-to-date information about risk analysis (Stollberg, Zhdanova, & Fensel, 2004). KBRR process represents all the experiences captured during the previous processes and stores them in a single computerized database as lessons learned and best practices. Additionally, KBRR serves as useful information for future risk analysis applicable to a wide variety of future projects (Karadsheh et al., 2008). Moreover, KBRR can provide support for information security RM personalization. A personalization strategy could prove useful to enable participants to find who knows what. In fact, personalization techniques are also valuable to support the discussions and negotiations between stakeholders (Papadaki & Polemi, 2008). Therefore, the repository can be linked to KBRC to assist in finding previous risks for a particular project or to find the right person with experience in dealing with certain type of risks. Moreover, KBRR serves as a real-time modification of the consequential risks by providing up to date

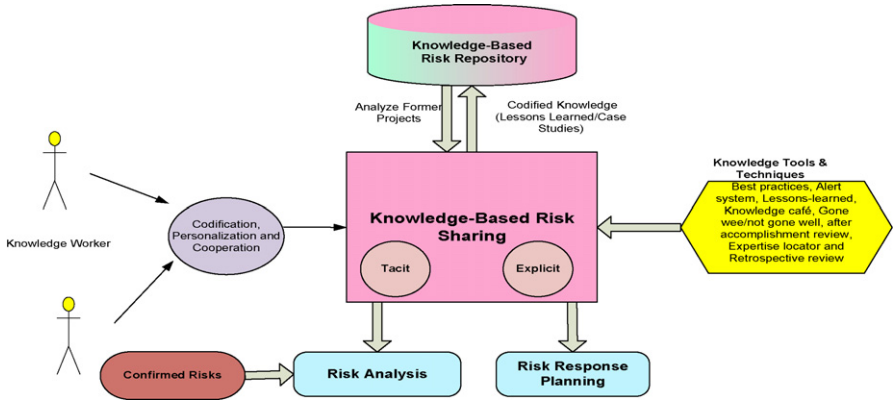


Fig. 10. Knowledge-Based Risk Sharing process.

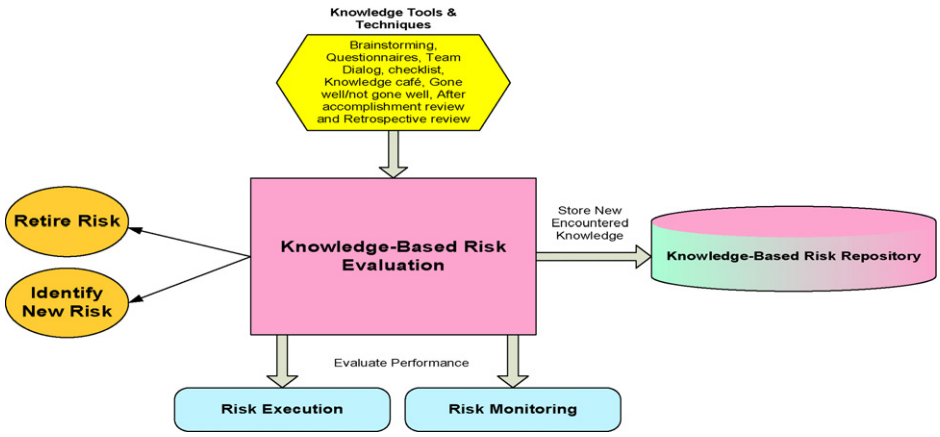


Fig. 11. Knowledge-Based Risk Evaluation process.

information for the project (Cornford, 1998). In risk monitoring, the real time monitoring of this process can help in modifying the risk execution process to maintain an update of the risks' list, which in turn is stored in the database of the KBRR system. If any new risk emerged during the software it will be referenced immediately through the database against previous similar projects to establish if there are previous lessons learned or best practices to assist in dealing with this risk efficiently. Therefore, the integration of knowledge database and risk database becomes essential to provide real time, update information to enable fast evolving in the face of environment changes (Karadsheh et al., 2008).

Also, KBRR can be considered as a knowledge warehouse which is collation of information captured, for example, from generic engineering know-how, lessons learned (in-depth internal expertise), case studies (internal and external case-based knowledge), best practices (external benchmarking) and engineering standards. The access to such knowledge means that the tool is capable of enabling the use of past successes and failures captured to minimize risks in project management (Kayis et al., 2007). The main components of the knowledge warehouse are (Kayis et al., 2007): (1) case studies based on specific projects were primarily used either through interviewing or capturing information and identifying critical success and failure factors; (2) lessons learned is in-house knowledge captured based on past experience because the success factor can be derived from historical lessons learned; 3) best practice transfer excellence from several sources into the organization, and also serves to populate the database with respect to identification of risk items and mitigation strategies. Fig. 12 illustrates the activities, input and output associated with KBRR process.

3.2.7.1. Knowledge update. Updating knowledge residing in the repository is an important task, and it can be assigned to a particular knowledge worker to maintain up-to-date information and to remove obsolete information (Karadsheh et al., 2009). The duties of knowledge workers are: updating knowledge or discovering and validating new knowledge, continuous validating and tuning of existing knowledge, retirement of obsolete knowledge, controlling and tracking the application of knowledge, and documenting and communicating of knowledge to affected business and technical staffs (Senator, 2000). Moreover, knowledge workers will ensure that any new knowledge is codified according to the organization's standard and in pre-designed template. This ensures that no knowl-

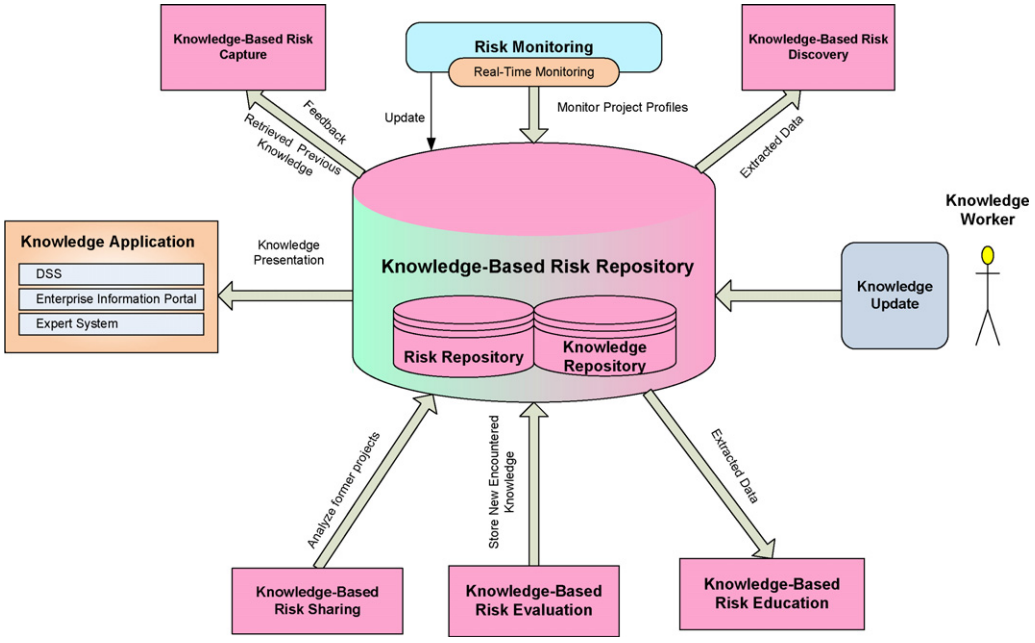


Fig. 12. Knowledge-Based Risk Repositories.

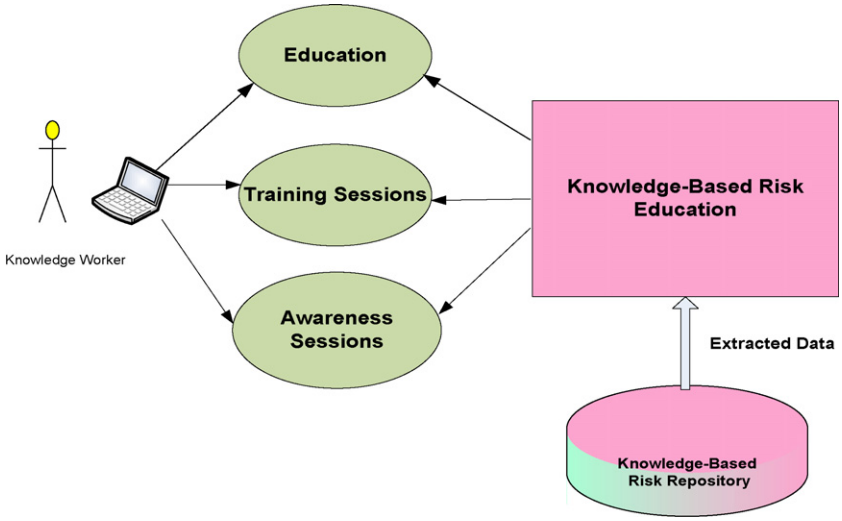


Fig. 13. Knowledge-Based Risk Education process.

edge is lost and the codified knowledge in the repository is updated for future projects.

3.2.7.2. Knowledge application. Selecting knowledge is an activity of extracting the knowledge from internal knowledge resources and providing it in a suitable representation to the users (Holsapple & Joshi, 2002) is an example of knowledge application. Therefore, Knowledge application provides a portal to access the latest information on the KBRR and updates to knowledge relevant to risks residing in the repository. ES, Decision Support System (DSS) and enterprise information portal are tools used to facilitate access. Building the enterprise data warehouse and performing data mining, statistics and analysis based on the implicit knowledge can be exercised through the excellent knowledge-base management system designed based on DSS as an example. The DSS can recognize as an efficient, safe and cooperated with KM and knowledge maintenance through the reasonable definition to the enterprise business process and organization structure as well as the employees' relationship (Liping, 2005). According to Papadaki and Polemi (2008) ES can be linked to the repository to allow users to easily find colleagues based on experience, interests or projects on which they work 3.2.8 Knowledge-Based Risk Education.

The stored knowledge of risk in the repository can be served as a training, education and awareness tool. As consequent, KBREdu access the repository for best practices Education and lessoned learned. Furthermore, KBREdu can provide a list of previous encountered risk for similar cases or projects. This process can be viewed as knowledge diffusion when the organization introduces the new knowledge to its operating environment (McElroy, 2000) through training and education. The purpose is to provide the training and the education to enhance the team's knowledge for future encountered situations that closely match a previous experience.

Moreover, any information identified, their handling and success of the treatments shall be reviewed periodically by the stakeholders and others in order to identify systemic project and organizational risks. Also, any individual project lessons may be gathered to help in identifying systemic risks ("Systems and software engineering – Life cycle processes – Risk management," 2006) and can serve as a learning and education tool for future projects.

Moreover, this process helps in providing training and education to deal with any risk that might occur in a future project and to avoid mistakes happened. According to Lengyel (2009) the concept of knowledge-based risk (KBRs) is defined as risk record, with associated knowledge objects, which provide a storytelling description of how risk was mitigated and what worked and what not. The goal is to transfer knowledge in risk context. This enables the team to review lessons captured to be able to answer questions such as, "What was the control and mitigation strategy?" Did it work? How were cost, schedule and technical performance affected?" This result in adding tacit knowledge to the individuals and make them better prepare for future projects. This process helps users utilizing the existing stored to generate and/or to produce an externalization of knowledge as process called Using Knowledge (Holsapple & Joshi, 2002).

Fig. 13 illustrates the activities, input and output associated with KBREdu process.

4. Conclusion

The aggressive competition has shaped the need for implementing new process to help the organization to succeed an IT projects. Consequently, the aim of this paper is to propose an integrated KM processes with RM processes and recommend a KBRM framework that solves the problem of an IT projects. The intent is to enhance the RRP (Risk Response Planning) process of risk identification, analysis, and execution by capturing the appropriate and relevant knowledge of risks based on the organization goals and objectives.

To the best of the author's knowledge there has not been a KM and RM integrated framework in the literature for mediating risks in an IT projects to explain the KBRC, KBRD, KBREx, KBRS, KBRE, KBRR, and KBREdu. This has encouraged the author to examine available studies from available sources. This paper adds to the body of knowledge of RM by providing a comprehensive framework and methodology for employing KBRM processes within IT organizations. Rather, understanding of the possible importance of risks, and commitment to their management, needs to be widespread throughout the organization. This, in most organizations, would require knowledge and knowledge management.

This research contributes to the understanding of the KM, RM and processes. The research has succeeded in proposing a framework which enriches current research by offering specification and justification of a set of interrelationships between important factors. As well, the research findings have met the aim of the research by proposing a conceptual framework of KBRM which describes the integration of KM and RM processes to improve RM for an IT projects. Consequently, this paper contributes by providing a clear

framework for employing KBRM as a framework to adapt to the hurried changing environment and sustain the business work. Future research would aim on developing a KBRM System, and implement the KBRM Framework as pilot studies in organizations.

It is hoped that the findings of this research will suggest an adequate level of interest from both the KM and RM communities in the field of IT, and encourage further investigation to address RM using KM tools and techniques, as discussed in this paper.

Future research would aim to preserve and improve the predictive power of the framework proposed in this research. At the end of this paper the following future research can be underline:

1. Develop Knowledge-Based Risk Management System.
2. Implement the Knowledge-Based Risk (RiskManIT) Framework as pilot studies in organizations.
3. Automate the KBRM (RiskManIT) approach.

References

Agostini, A., Albolino, S., Michelis, G. D., Paoli, F. D., & Dondi, R. (2003). Stimulating knowledge discovery and sharing. In *Paper presented at the proceedings of the 2003 international ACM SIGGROUP conference on supporting group work* Sanibel Island, Florida, USA.

Alavi, M., & Leidner, D. (1999). Knowledge management system: issues, challenges, and benefits. *Communications of the Association Information System*, *1*(7).

Alhawari, S., Thabath, F., Karadsheh, L., & Hadi, W. (2008). A risk management model for project execution. In *Paper presented at the 9th IBIMA conference information management in modern organizations* Marrakech, Morocco.

Alryalat, H., & Alhawari, S. (2008). Towards customer knowledge relationship management:: integrating knowledge management and customer relationship management process. *Journal of Information & Knowledge Management*, *7*(3), 145–157.

Baccarini, D., Salm, G., & Love, P. (2004). Management of risks in information technology projects. *Industrial Management & Data Systems*, *104*(4), 286–295.

Becerra-Fernandez, I., Gonzalez, A., & Sabherwal, R. (2004). *Knowledge management: Challenges solutions and technologies (Har/Cdr ed.)*. Upper Saddle River, New Jersey: Prentice Hall Inc.

Beck, M., Drennan, L., & Higgins, A. (2002). *Managing E-Risk*. London: Association of British Insurers.

Bernanke, B. (2009). The economic outlook. Retrieved from: http://www.federalreserve.gov/newsevents/testimony/bernanke20090505a.htm

Bruckner, M., List, M. B., & Schiefer, J. (2001). Risk-management for data warehouse systems. *Lecture Notes in Computer Science*, *2114*, 219–229.

Caldwell, F. (2008). Risk intelligence: Applying KM to information risk management. *Journal of VINE*, *38*(2), 163–166.

Chan, I., & Chao, C. (2008). Knowledge management in small and medium-sized enterprise. *Communication of the ACM*, *51*(4).

Cornford, S. (1998). Managing risk as a resource using the defect detection and prevention process. In *Paper presented at the international conference on probabilistic safety assessment and management* New York, 13–14 September.

Carbone, T., & Tippett, D. (2004). Project risk management using the project risk FMEA. *Engineering Management Journal*, *16*(4), 28–35.

Cule, P., Schmidt, R., Lyyttnen, K., & Keil, M. (2000). Strategies for leading off is project failure. *Information Systems Management*, *14*(2), 68–73.

Davenport, T. H., & Prusak, L. (1998). *Working knowledge-how organizations manage what they know* (1st ed.). Boston, MA: Harvard Business School Press.

de Rezende, J. L., & de Souza, J. M. (2007). Using knowledge management techniques to improve the learning process through the exchange of knowledge chains. In *Paper presented at 11th International conference on the computer supported cooperative work in design, 2007 (CSCWD 2007)*.

Del Cano, A. D., & Cruz, M. P. (2002). Integrated methodology for project risk management. *Journal of Construction Engineering and Management*, *128*(6), 473–485.

Farias, L., Travassos, G., & Rocha, A. (2003). Managing organizational risk knowledge. *Journal of Universal Computer Science*, 103–110.

Fayda, S. N. A., Ulusoy, G., & Meyanli, I. (2003). Design of post project analysis and risk management processes for R&D projects.

Fuller, M. A., Valacich, J. S., & George, J. F. (2008). *Information systems project management: A process and team approach* (1st ed.). Prentice Hall.

Goh, A. (2005). Adoption of customer relationship management (CRM) solutions as an effective knowledge management (KM) tool: A systems value diagnostic. *Journal of Knowledge Management Practice*, 6.

Gold, A. H., Malh otr a, A., & Segar s, H. (2001). Knowledge management: An organizational capabilities perspective. *Journal of Management Information Systems*, *18*(1), 185–214.

Higuera, R. P., & Haimes, Y. Y. (1996). *Software Risk Management*. Pittsburgh, PA: Carnegie Mellon University.

Holsapple, C. (2005). The inseparability of modern knowledge management and computer-based technology. *Journal of Knowledge Management*, *9*(1), 42–52.

Holsapple, C. W., & Joshi, K. D. (2004). A formal knowledge management ontology: conduct, activities, resources, and influences. *Journal of American Society for Information Science and Technology*, *55*(7), 593–612.

Holsapple, C., & Joshi, K. (2002). Knowledge management: A three-fold framework. *The Information Society*, *18*(1), 47–64.

Jennex, M. E. (2005). The issue of system use in knowledge management systems. In *Paper presented at the Proceeding of the 38th Hawaii conference on system sciences*.

Jones, H. (2005). Risking knowledge management: an information audit of risk management activities within the Hobart city council. *Journal of Library Management*, *26*(6/7), 397–407.

Kahn, B., & Adams, E. (2000). Sales forecasting as a knowledge management process. *The Journal of Business Forecasting*, 19–22.

Karadsheh, L., Alhawari, S., El-Bathy, N., & Hadi, W. (2008). Incorporating knowledge management and risk management as a single process. In *Proceedings of International Conference of the Global Business Development Institute (GBDI)* Las Vegas, NV, USA, pp. 207–214.

Karadsheh, L., Mansour, E., AlHawari, S., Azar, G., & El-Bathy, N. (2009). A theoretical framework for knowledge management process: towards improving knowledge performance. *Journal of Communications of the IBIMA*, *7*, 67–79.

Kasap, D., & Kaymak, M. (2007). Risk Identification Step of the Project Risk Management. In *Management of Engineering and Technology. Paper presented at the Portland International Center for Portland* Oregon, USA.

Kayis, B., Zhou, M., Savci, S., Khoo, Y. B., Ahmed, A., & Kusumo, R. (2007). IRMAS-development of a risk management tool for collaborative multi-site, multi-partner new product development projects. *Journal of Manufacturing Technology Management*, *18*(4), 387–414, doi:10.1108/17410380710743770.

Kim, K., Lim, S., & Mitchell, B. (2004). Building a knowledge model: A decision-making approach. *Journal of Knowledge Management Practice*, 5.

Lengyel, D. (2009). Integrating risk and knowledge management for the exploration systems mission directorate. *Academy Sharing Knowledge Ask Magazine*.

Liping, S. (2005). Decision support systems based on knowledge management. In *Paper presented at the Services systems and services management, 2005. Proceedings of ICSSSM'05* , 2005.

Malhotra, Y. (2005). Integrating knowledge management technologies in organizational business processes: Getting real time enterprises to deliver real business performance. *Journal of Knowledge Management*, *9*(1), 7–28.

Massingham, P. (2010). Knowledge risk management: A framework. *Journal of Knowledge Management*, *14*(3), 464–485.

Marin-Garcia, J., & Zarate Martínez, E. (2007). A theoretical review of knowledge management and teamworking in the organizations. *International Journal of Management Science and Engineering Management*, *2*(4), 278–288.

McElroy, M. (2000). Integrating complexity theory, knowledge management and organizational learning. *Journal of Knowledge Management*, *4*(3), 195–203.

Mees, W. (2007). Risk management in coalition networks. In *Third international symposium on information assurance and security* (pp. 329–336).

Nehari-Talet, A., Alhawari, S., & Alryalat, H. (2010). The effect knowledge process on customer knowledge expansion. *The International Journal of Knowledge Culture and Change Management*, *10*(2), 181–200.

Miles, F. M., & Wilson, T. G. (1998). Managing project risk and the performance envelope. In *Proceedings of the 13th annual applied power electronics conference and exposition, APEC* Singapore, February, (pp. 15–19).

Michael, S., Zhdanova, A., & Fensel, D. (2004). H-TechSight a next generation knowledge management platform. *Journal of Information and Knowledge Management*, *3*(1), 47–66.

Miltiadis, L., Pouloudi, A., & Poulymenakou, A. (2002). Knowledge management convergence expanding learning frontiers. *Journal of Knowledge Management*, *6*(1), 40–51.

Neef, D. (2005). Managing corporate risk through better knowledge management. *Journal of The Learning Organization*, *12*(2), 112–124.

Olsson, R. (2008). Risk management in a multi-project environment; an approach to manage portfolio risks. *The International Journal of Quality and Reliability Management*, *25*(1), 60–71.

wen, J. (2006). Integrating knowledge management with programme management. *International Journal of Knowledge Management*, *2*(1), 41(17).

Padayachee, K. (2002). An interpretive study of software risk management perspectives. In *Paper presented at the Proceedings of SAICSIT*.

Papadaki, K., & Polemi, D. (2008). Collaboration and knowledge sharing platform for supporting a risk management network of practice. In *Paper presented at the Third international conference on internet and web applications and services*.

Pentland, T. (1996). Information systems and organizational learning: The social epistemology of organizational knowledge systems. *Accounting, Management and Information Technologies*, *5*(1), 1–21.

Perera, J., & Holsomback, J. (2005). An integrated risk management tool and process. In *Paper presented at the Aerospace conference, 2005 IEEE*.

Project Management Institute, I. (2004). *A guide to the project management body of knowledge: PMBOK guide* (3rd ed.). Project Management Institute. (p. 380).

Qi, L. (2008). Advancing knowledge discovery and data mining. In *Paper presented at First international workshop on the knowledge discovery and data mining, 2008 (WKDD 2008)*..

A Risk Management Standard. (2002). Retrieved from http://www.theirm.org/publications/PUstandard.html

Rodriguez, E., & Edwards, J. (2008). Before and after modeling: Risk knowledge management is required. In *Paper presented at the 6th Annual premier global event on ERM, Chicago, IL*.

Roy, G. (2004). A risk management framework for software engineering practice. In *Paper presented at the Software engineering conference, 2004. Proceedings, Australian*.

Sallmann, F. (2007). *Knowledge-based risk management*. VDM Ver lag Dr. Mueller e. K.

Scott, A. (2002). Your say: Managing knowledge to manage risk. *Inside Knowledge*, *6*(1). Retrieved from: http://www.ikmagazine.com

Schwalbe, K. (2007). *Information technology project management* (5th ed.). Course Technology, Thomson Learning.

Senator, T. E. (2000). Ongoing management and application of discovered knowledge in a large regulatory organization: A case study of the use and impact of NASD Regulation's Advanced Detection System (RADS). In *Paper presented at the Proceedings of the sixth ACM SIGKDD international conference on knowledge discovery and data mining* Boston, Massachusetts, United States.

Shaw, J. (2005). Managing all your enterprise's risk. *Risk Management*, *52*, 85–94.

Senator, T. E. (2005). Link mining applications: progress and challenges. *SIGKDD Exploration Newsletter*, *7*(2), 76–83. http://doi.acm.org/10.1145/1117454.1117465

Stonebumer, G., Goguen, A., & Feringa, A. (2002). Risk management guide for information technology systems. 800-30, 54.

Stollberg, M., Zhdanova, V., & Fensel, D. (2004). H-TechSight – A next generation knowledge management platform. *Journal of Information and Knowledge Management*, *3*(1), 47–66.

Sun, Z., & Gang, G. (2006). HSM: A hierarchical spiral model for knowledge management. In *Paper presented at the Proceedings of 2nd international conference on information management and business* Sydney, Australia.

Sunassee, N. N., & Sewry, D. A. (2002). A theoretical framework for knowledge management implementation. In *Paper presented at the Proceedings of the 2002 annual research conference of the South African institute of computer scientists and information technologists on enablement through technology* Port Elizabeth, South Africa.

Systems and software engineering – Life cycle processes – Risk management. (2006). Std ISO IEC 16085 – 2006, c1–36.

Tah, J., & Carr, V. (2001). Knowledge-based approach to construction project risk management. *Journal of Computing in Civil Engineering*, *15*, 170–177.

Tesch, D., Kloppenborg, T., & Frolick, M. (2007). IT project risk factors: The project management professionals perspective. *Journal of Computer Information Systems*, *47*(4), 61–69.

Dr. Samer Alhawari has a PhD in Management Information Systems from the Arab Academy for Banking and Financial Sciences, Amman-Jordan. He is an assistant professor in the Department of Management Information System at the Applied Science Private University, Jordan. His research interest includes Knowledge Management, Customer Relationship Management, Customer knowledge Management, Risk Management, Strategic Management, Information Systems, Data mining, and Text Categorization. Dr. Alhawari has published 33 articles in refereed journal as well as national and international conference proceedings.

Dr. Louay Karadsheh has a Doctorate of Management in Information Technology from Lawrence Technological University, Southfield, MI. He is an assistant professor in Computer Information System department at ECPI University. His research interest includes Cloud Computing, Information Assurance, Knowledge Management and Risk Management. Dr. Karadsheh has published eight articles in refereed journals and international conference proceedings and has extensive knowledge in operating system, networking and security.

Dr. Amine Nehari-Talet is an Associate Professor, MIS KFUPM, teaching undergraduate and postgraduate courses (MBA and EMBA), 23 years teaching experience in higher education. He has authored 50 articles in Information Systems, E-learning and knowledge Management refereed journals and international conference proceedings. He is member International Association for Computer Information Systems (IACIS) editorial for many Journals, and IBIMA Conference Advisory Committee. He has been awarded a certificate on Online teaching from University Illinois October 2005, a Certificate of completion "Oracle Database 11g: Administration Workshop I" March 2009 "Oracle 9i Designer: First Class" June 2009 Oracle University.

Dr. Ebrahim Mansour is an Assistant Professor and Head of MIS Department at Applied Science University, Amman, Jordan. He has a PhD in Financial Information Systems from Brunel University, London, UK. Dr Mansour research Interest includes but not limited to Financial and Accounting Information Systems, Knowledge Management, Decision Support Systems, E-Business and Simulation. Dr. Mansour has published more than 10 articles in refereed journal as well as national and international conference proceedings.