The Role of Knowledge Management with Risk Management for Information Technology Projects Risk Assessment

Amine Nehari Talet*
Department of Accounting & MIS, King Fahd University of Petroleum & Minerals, Saudi Arabia

Abstract. Information technology projects management is not free from risks, which are created from various sources of the environment; they are not just related to financial aspects. Information technology is now omnipresent in the lives of people across the globe. Information technology, as a technology with the fastest rate of development and application in all branches of business, requires adequate consideration of risk assessments. The risks faced by IT projects are not, in essence, financial risks. By understanding these fundamental problems in real terms, rather than through their financial impact, IT project managers can move more quickly to resolve issues before they become major problems that threaten the goals of the project. This paper will focus on how lack of knowledge management support for risk management processes has caused many project failures in the past.

These technologies take many forms such as personal computers, smartphones, the internet, web and mobile phone applications, digital assistants, and cloud computing. In fact, the list is growing constantly and new forms of these technologies are working their way into every aspect of daily life. Thus, a complete understanding of these possible risks and creating strategic policies to challenge them are one of the fundamental requirements for successful implementation of IT projects.

Keywords. knowledge management, risk management, risk

Introduction

The risks faced by IT projects are not, in essence, financial risks. By understanding these fundamental problems in real terms, rather than through their financial impact, IT project managers can move more quickly to resolve issues before they become major problems that threaten the goals of the project. In order to minimize losses, it is necessary to involve risk management and risk assessment in the areas of information technology and operational risks.

There are various definitions of Risk Management and Risk Assessment ISO 13335 (ISO 13335-2; European Network and Information Security Agency [ENISA], 2006), but most experts accept that Risk Management involves analysis, planning, implementation, control and monitoring of implemented measurements, and Risk Assessment, as part of Risk Management.

According to the current project management literature, the achievement of IT projects is influenced by risks and risk management (Didraga, 2013), the management of risks in projects is a growing area of interest. Aloini et al. (2012) concluded that risk management could lead to a range of benefits for both projects and organizations. It provides guidance for decision-making regarding alternative options for a project, increases confidence in the success of a project, and reduces the risk of unexpected events that can cause delays and excess expenditures.
Risk management (RM) is the identification, assessment, and prioritization of risks followed by the coordinated and economical application of resources to reduce, monitor, and control the possible impact of unfortunate events or to maximize the realization of opportunities (Lee, 2014). In another study, risk management could be used to increase the success level of new product development projects due to their highly complex nature (Porananond and Thawesaengkulthai, 2014). Recently, Denas (2015) noted that since 2000, the publication of papers on risk ranking and analysis has increased, especially concerning multicriteria decision-making techniques.

Risk management in the creation of projects is full of deficiencies that affect its efficiency as a project management goal and, in the end, the project’s performance (Serpellaa et al., 2014).

Risk management recognizes risk, accesses risk, and takes measures to reduce risk, as well as measures for risk maintenance on an acceptable level. The main aim of risk assessment is to make a decision on whether a system is acceptable, and which measures would provide its acceptability.

For every organization using IT in its business process, it is significant to conduct the risk assessment. Numerous threats and vulnerabilities are presented and their identification, analysis, and evaluation enable evaluation of risk impact, and proposing of suitable measures and controls for its mitigation on the acceptable level.

The Role of Knowledge Management Process in Project Risk Management

The project risk management process, as described in project management handbooks, is an example of a rational problem-solving method (Kutsch and Hall, 2005) based on an instrumental view. For this process to be effective, it is necessary to follow all prescribed steps as shown in Figure 1.

For example, it has been have shown that the prescribed sequence of risk identification, risk analysis, planning actions, and executing actions is rarely followed (Bannerman, 2008; Voetsch et al., 2004). 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 (Bakker et al., 2010). Nevertheless, project managers often choose to execute various risk management activities in their projects (Bannerman, 2008; Voetsch et al., 2004) in order to manage their risks and uncertainties (Knight,
1921). 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.

Knowledge management (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 environments, 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 (Massingham, 2010). Individuals not knowing enough about the risk to anticipate its likelihood and consequences manifest the problem of environmental complexity. 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 the KM processes.

KM processes can be generally characterized as including of knowledge creation activities and knowledge transfer activities (Hurley and Green, 2005).

Based on research conducted by Rodriguez and Edwards (2008), an effective RM process model cannot be achieved without the assistant of a well-established KM process model. Therefore, a well-defined and designed integrated KM and RM framework is essential to improve decision-making in IT projects. 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 (Shaw, 2005).

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. A number of business and academic gurus have said that in order for organizations to have a lasting competitive advantage, they will have to be knowledge driven (Holsapple and Josh, 2002). KM processes have also turned out to be strategic resources for organizations. KM can have a great influence on reducing organizations' risks (Karadsheh et al., 2009). 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.

According to Neef (2005), a company cannot manage its risks effectively if it cannot manage its knowledge. Many projects fail 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 et al., 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).

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 (Owen, 2006); 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.

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 with an accurate and timely information about potential harmful incidents, for example (Neef, 2005). 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. This pilot audit has improved the understanding and application of information and KM in the Council (Jones, 2005). 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 (Caldwell, 2008). 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 (Caldwell, 2008).

Figure 2: Knowledge Management Acts through Risk Modeling in Different Components of Enterprise Risk Management Processes (Rodriguez and Edwards, 2008)
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 and Holsombok, 2005). Our proposed KBRM framework for an 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-modeling knowledge was introduced to improve the quality and quantity of RM processes. As shown in Figure 2, Rodriguez and Edwards (2008) claimed that in three key components of Enterprise Risk Management (ERM), 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 it is 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; and (7) connecting organizational performance metrics and risk modeling.

Another interesting research in managing knowledge risks is described by Tah and Carr (2001), in which they present 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 comprehensive RM tool is called IRMAS (Intelligent Risk Mapping and Assessment System). This RM tool contains some KM tools and techniques (Kayis et al., 2007). 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 an 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 abovementioned 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.

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.

There are varieties of RM processes used in organizations today. These are summarized in Table 1.

### Knowledge Management and Risk Identification

Organizational risk management (RM) is a complex and important task for managers, particularly as the consequence of poor RM is becoming observable through financial loss.
Managers must be aware of the risks related with their organization’s activities and have in place ways to manage unwanted events. RM has become the main part of the organization’s activity and its main objective is to help all other activities to reach the organization’s aim directly and efficiently. RM is a continuous process that depends directly on the change in the internal and external environment and requires continuous attention for identification and control of risk (Tchankova, 2002).

Shao and Wu (2010) proposed that an integrated risk management model for financial banks with knowledge management considers the risks before a project or an investment, assesses and calculates the risks using all kinds of ways, adjusts the operation according to the changeable environment, and feeds back timely. They recommend that the financial banks should set up the incentive mechanism to urge the staff to learn more knowledge, and at the same time, banks should train knowledgeable staff to construct a

Table 1
The processes of RM in a number of existing process models in the area of RM

<table>
<thead>
<tr>
<th>Main Dimension/ RM Process</th>
<th>Description of Process</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software development process</td>
<td>Risk identification</td>
<td>Risk analysis</td>
<td>Risk control planning</td>
<td>Risk monitoring</td>
<td>(Boehm and Bose, 1994)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Software risk management</td>
<td>Risk Identification</td>
<td>Risk Analysis</td>
<td>Risk Plan</td>
<td>Risk</td>
<td>Risk Control</td>
<td>(Higuera and Haimes, 1996)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Role in software engineering</td>
<td>Risk Identification</td>
<td>Risk Analysis</td>
<td>Risk Control Planning</td>
<td>Risk Analysis</td>
<td>Risk Control</td>
<td>(Kontio, 1997)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RM as verification and validation</td>
<td>Risk Identification</td>
<td>Risk Analysis</td>
<td>Risk Planning</td>
<td>Risk Tracking</td>
<td>Risk Control</td>
<td>(Cornford, 2001)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Software project management</td>
<td>Risk Identification</td>
<td>Risk Analysis</td>
<td>Risk Prioritization</td>
<td></td>
<td></td>
<td></td>
<td>(Jurison, 1999)</td>
<td></td>
</tr>
<tr>
<td>Software development</td>
<td>Risk Identification</td>
<td>Risk analysis</td>
<td>Risk monitoring</td>
<td></td>
<td></td>
<td></td>
<td>(Bandyopadhyay et al., 1999)</td>
<td></td>
</tr>
<tr>
<td>Data warehouse system</td>
<td>Goal definition</td>
<td>Risk Identification</td>
<td>Risk Analysis</td>
<td>Risk Planning</td>
<td>Risk Tracking</td>
<td>Risk Control</td>
<td>(Bruckner et al., 2001)</td>
<td></td>
</tr>
<tr>
<td>Controlling product development</td>
<td>Identify Risks</td>
<td>Analyze Risks</td>
<td>Prioritize Risks</td>
<td>Resolve Risks</td>
<td></td>
<td></td>
<td>(Smith, 2002)</td>
<td></td>
</tr>
<tr>
<td>Project management</td>
<td>RM planning</td>
<td>Qualitative risk analysis</td>
<td>Quantitative risk analysis</td>
<td>Risk response planning</td>
<td>Risk monitoring and control</td>
<td></td>
<td>(Project Management Institute, 2008)</td>
<td></td>
</tr>
<tr>
<td>Software engineering</td>
<td>Risk Identification</td>
<td>Risk Analysis</td>
<td>Risk Planning</td>
<td>Risk Monitoring</td>
<td></td>
<td></td>
<td>(Sommerville, 2006)</td>
<td></td>
</tr>
<tr>
<td>Software Risk Management Process</td>
<td>Plan and implement risk management</td>
<td>Manage the project risk profile</td>
<td>Perform risk analysis</td>
<td>Perform risk monitoring</td>
<td>Perform risk treatment</td>
<td>Evaluate RM process</td>
<td>(Society, 2006)</td>
<td></td>
</tr>
<tr>
<td>Risk architecture</td>
<td>Risk classification</td>
<td>Risk identification</td>
<td>Initial risk assessment</td>
<td>Risk mitigation</td>
<td>Risk monitoring</td>
<td></td>
<td>(TOGAF, 2009)</td>
<td></td>
</tr>
</tbody>
</table>
whole system to assess and calculate the potential risks and countermeasures to reduce risks and feedback.

The literature of knowledge management recognizes the importance of two concepts: (1) relating knowledge management to business goals, and (2) analyzing 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 (Jones, 2005). The new field of knowledge risk management (KRM) offers managers ways to use knowledge to make sure decision-makers are informed and can anticipate and respond to risk events (Massingham, 2010).

Risk identification (RI) is the first step in the proactive RM process. It provides the opportunities, indicators, and information that allow an organization to raise major risks before they adversely affect operations and then the business determines the strategy to address them throughout the transformation. Project managers can take appropriate action if proper risk assessment leads to early identification of a failing project.

Risk identification covers the identification within the established context of uncertain events that could cause harm or benefit associated causes and the potential consequences (Williams et al., 2006). 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 (Holm, 2001).

A case study research was conducted to strengthen KM strategies by using RM as a function of governance (Zyngier, 2008). This can be ensured through developing RM reporting templates and procedures to guarantee appropriate feedback into the KM system. In other words, RM can be used as an organized feedback to deal with cultural and structural risk factors to KM policy. Additionally, KRM is an emerging field, which offers a solution to the problems related with conventional risk management methods. Individuals not knowing enough about the risk to anticipate its likelihood and consequences manifest the problem of environmental complexity and it creates uncertainty (Massingham, 2010).

The globalization and the technological development in the business sector forces business organizations to cooperate on a broader scale. The knowledge of cooperation and the risks into cooperation have become fundamental to business success (Ehrengren, 2011). In addition, correct risk identification ensures risk management effectiveness. A project failure can be the result of capturing the appropriate knowledge at an inappropriate time of the project (Fuller et al., 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). It appears that is not sufficient to augment current Information Security Risk Assessment (ISRA) methodologies merely by including the identification of “knowledge assets” in the form of databases, or even key people (Shedden et al., 2009).

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 (Shedden et al., 2009). Information security is 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 (Braber et al., 2007).

Therefore, risk intelligence is the alignment of information governance and information risk management to business priorities. Not only does this alignment help mitigate the risks to business goals, but it also leads to direct savings in legal and compliance costs, especially when
knowledge management (KM) principles are applied.

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; and (4) risk monitoring: to guarantee the effectiveness of the methods followed and to monitor the risks throughout the project (Sommerville, 2006).

In addition, in the 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: (1) basic database, (2) knowledge database management, (3) supply chain risk early warning, and (4) risk management strategies module (Bing-hua and Guo-fang, 2009).

Knowledge Management and Risk Analysis

In the analysis of risk management (RM) of the organizations, the first process is the risk assessment that, with attention to link the risk to the IT system throughout the software development life cycle (SDLC), this process is used to determine the danger of minimal risk. Output of this process also helps identify the technical controls to reduce or limit the risk during the process of risk reduction. To determine the likelihood of future adverse events, analyzing vulnerability and potential threats to IT systems is essential. According to Maguire (2002), 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. Maguire 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 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. Therefore, with RM, the elements of risk have to be isolated at early stages resulting in more projects that are successful and fewer chances of failure.

Risk analysis facilitates the conversion of risk data into decision-making information (Higuera and Haimes, 1996). Each risk identified in the previous stage will be analyzed in this process. Risk analysis 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; and (4) for each risk that is above its risk threshold, recommended treatment strategies shall be defined and documented as recommended by the 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 extent 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, and (3) displays the
extent of loss to determine the risk disclosure in order to list all risks and threats (Karadsheh et al., 2008).

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 (Society, 2006). Also, risk analysis will categorize the risks based on the likelihood of occurrence, impact, and extent of loss (Higuera and Haimes, 1996). Also, in the 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 (Society, 2006).

Knowledge sharing plays an important role in enriching the risk analysis process with tacit and explicit knowledge. The project team shares their experience by performing analysis on each identified risk. The project team meets to exchange their thoughts and experience on which method might be appropriate in executing the risk analysis process. The team members will discuss their experience on confirmed risks based on probability of occurrence, impact, and extent of loss. Techniques for risk analysis include (Karadsheh et al., 2008):
- Best practice, alert system, and lessons-learned.
- Expertise locator might be needed to share tacit and explicit knowledge.
- Risk modeling to transfer knowledge through presentation, portals, discussions, collaboration activities, and testing reporting.
- Review case studies from previous projects.
- Quick evidence review (QER) to review research and evidence on a particular issue.
- Gone well/not gone well tools.
- Team discussion and brainstorming performed by analyzing former projects accessed from the repository.

Another research examining the relationship between knowledge and risk analysis is described by Tah and Carr (2001). 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.

Another example of the integration of KM elements with RM is user involvement (Spears, 2006). Spears stated that user contribution is vital to recognizing information security risks in repetitive business processes because they possess detailed knowledge of business processes. His research develops a theory of the consultative form of user participation that emphasizes the cognitive benefits of user participation. In consultative participation, designated users acting as subject matter experts with detailed knowledge of specific business processes participate in a risk analysis to identify information security vulnerabilities. He expected that previously unknown information risks will be identified, thereby increasing the quality of information used for information risk management. Furthermore, knowledge of identified risks is expected to be transferred between peers or other participant groups (e.g., IT), which is expected to ultimately lead to improved information security through enhanced policies and procedures. The output of the risk analysis process is a detailed description of every valid risk, severity, impact, priority, probability, and impact estimates.
Knowledge Management 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 (Higuera and Haimes, 1996). 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 (Bruckner et al., 2001). 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 the Project Management Institute (2004), 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.

Risk response planning turns risk information into decisions and actions. 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 (Bruckner et al, 2001); (2) reduction of magnitude of loss; or (3) change of the consequence of a risk (Bruckner et al., 2001). The process output, accordingly, are simple rules, process controls, testing, modeling, and inheritance to (Beck et al., 2002).

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 (Society, 2006). Moreover, knowledge sharing helps the team in the 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 (Faria et al., 2003). Once stakeholders reach an agreement on which risk treatment is accepted, a detailed treatment plan should be defined on how it is to be executed.

Also, during this stage, the reporting and communication is established to the stakeholders. There will be internal and external reporting. The purpose is to share the knowledge obtained during the execution process (IRM, 2002):

- Internal reporting: different levels within an organization need different information from the RM process.
- External reporting: a company needs to report to its stakeholders on a regular basis setting out its RM policies and the effectiveness in achieving its objectives.

Knowledge sharing plays a vital role in establishing a collaborative environment that fosters the exchange of knowledge during IT projects. This might result in enhancing RM execution by reducing lost time in search for an answer, faster learning, and efficient executions of activities during certain RM processes.
Knowledge Management and Risk Monitoring

If a risk event occurs during project execution, there is a likelihood it was identified sometime earlier, it was analyzed, and an appropriate response action was planned to deal with it (captured in the Risk Register). For the most part, Risk Monitoring and Control is the process of putting into action all of the risk planning done earlier in the project life cycle. It is important to understand that risk monitoring is intended to be a daily, ongoing process across the entire project life cycle. 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. The Risk Monitoring and Control process is applied to:

1. Monitor identified risks.
2. Identify new risks.
3. Ensure proper execution of planned risk responses.
4. Evaluate overall effectiveness of the risk management plan in reducing risk.

In this process, risk monitoring is viewed as a feedback process for reevaluating recent results of risk execution concerning certain risk. The purpose of risk monitoring is to (Society, 2006):

1. Review and update the individual risk states and the RM context.
3. Seek out new risks and sources.

In addition, 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 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 (Tah and Carr, 2001). Removing the risk from the project does not mean no documentation is performed for future reference.

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 (Project Management Institute, 2004).

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 (Perera and Holsumback, 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 (Project Management Institute, 2004).

Additionally, the team will meet to assess the risk project performance and to exchange their knowledge accordingly. The purpose is to share their experience and assess the outcome. According to systems and software engineering—life cycle processes—risk management (Society, 2006), three steps are important to monitor risk performance:

1. Monitor risk throughout the life cycle for changes in their 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. 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.

(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.

Any monitoring 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 the Institute of Risk Management (IRM, 2002).

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 the RM project. The first process is Risk Identification, which is the process of identifying the threats on the business. The threats according to security taxonomy are strategic risks, operational and systems risks, legal and regulatory risks, and financial risks. The second process is a Risk Evaluation to produce a list of all possible threats to the e-business in relation to the likelihood and their severity. The third process is Risk Control, which is deciding the best suitable and cost-effective measures needed to be executed in order to control the risks. Such measures may involve Risk Avoidance, Risk Reduction, and Risk Transfer. The fourth process is Risk Monitoring, which provides a review of the organization’s ability to deal with incidents that might result in business interruption, implementing Risk Identification, Evaluation and Control measures that minimize the likelihood and severity—both in terms of potential financial and reputation losses of an incident, but can eliminate the risks.

The RM process is divided into Risk Identification, which results in a variety of technological content, environmental communications, the execution and operation approaches, programmatic constraints, and the mission duration (Cornford, 2001). The second is Risk Analysis of the consequences of the possible risks by scoring their impact on the necessities should they occur. The result is a requirement-driven risk list where failures are listed based on their impact on weighted requirements. The risk planning process has the following design rules: process controls, testing, modeling, and inheritance. Risk Tracking contains a tool to display the number of report formats to be used by dissimilar personnel for different reasons. Risk Control is designed for implementation. This allows the project team to effectively control risk and watch its growth or decline as the design evolves and the results of implementation become available.

The RM process is described in six steps:

1. Goal Definition: review the stated goals for the project, refine them, and define implicit goals and constraints explicitly.
2. Identification: identify potential threats to the project using multiple approaches.
3. Analysis: classify risks, complete risk scenarios, estimate risk effects, estimate probabilities, and utility losses for risk scenarios.
4. Control and Planning: select the most important risks, propose controlling actions and the actions for implementation.
5. Control: implement the risk controlling actions.
6. Monitoring: monitor the risk situation (Kontio, 1997).

Figure 3 illustrates the proposed Riskit method by (Kontio, 1997).

The RM process contains the following processes:

1. Identifying risks using brainstorming techniques to discover any risks that prevent the progress of the project.
2. Analyzing risks by the team members to determine if a certain risk is worth migrating or not.
3. Prioritizing and mapping risk to establish a seriousness of the risk according to their impact.
(4) Resolving risks by implementing plans to prevent risk from occurring (Smith and Merritt, 2002).

RM involves 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; and (4) Risk Monitoring to guarantee the effectiveness of the methods followed and to monitor the risks throughout the project. Figure 4 illustrates the RM process (Sommerville, 2001).

![Figure 3: Riskit RM Cycle (Kontio, 1997)](image-url)
Sources of Risks in IT Projects

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

IT projects are characterized by high degrees of risk. The rapid pace of change in technologies combines changes in business processes to create unpredictable shifts in cost, the cost-benefit relationship, and the feasibility of doing specific things in particular ways (Schwalbe, 2007). One classic problem identified in many IT projects occurs when new technologies are developed as the project is underway (Havenstein, 2007).

A survey of more than a thousand Canadian organizations found that the main reason for IT project failure was inadequate risk management and a weak project plan. The risks faced by IT projects are not, in substance, financial risks (Whittaker, 1999). The financial measures are only indicators of the underlying problems. By understanding these underlying problems in real terms, rather than through their financial impact, IT project managers can move more quickly to resolve issues before they become major problems that threaten the goals of the project.

Most IT practitioners understand that there are risks other than financial risk in projects. IT project risk can be broken into nine categories, including financial risk, technology risk, security risk, information risk, people risk, business process risk, management risk, external risk, and even the risk of success—which occurs when the project is so well done that it draws more transactions than expected and fails to scale to the overload requirements (McKeen and Smith, 2003).

Anecdotes, surveys, and field research studies establish that many IT projects fail. Managers abandon some of these failing systems. Other projects that are over budget or behind schedule ultimately result in useful systems (Anthes, 1993). However, many more projects continue long after any hope of success has faded (Johnson, 1995; Newman, 1996). IT projects are much more likely to fail than other types of projects, such as building construction projects and Schneider (2009) states that the main causes for IT project failures are their use of rapidly changing technologies, their generally long development times, and the volatility of user expectations about what the project will yield. Because IT projects generally include all of these characteristics, they are prone to failure, cost overruns, and schedule delays.

Organizations need to keep IT projects on schedule and costs under control. However, organizations must also encourage managers to respond to changing business needs and exploit technological opportunities before their competitors do so (Murthi, 2002). In terms of IT projects, risks can vary, whether it is a software development project, security project, outsourcing project, or specific programming task.

IT projects are known for their high failure rate. In-depth interviews with IT professionals from leading firms in Western Australia were undertaken to determine how IT risks were managed in their projects. The respondents ranked 27 IT risks in terms of likelihood and consequences to identify the most important risks (Baccarini, 2004). The top five risks, in order, were personnel shortfalls; unreasonable project schedule and budget; unrealistic expectations; incomplete requirements; and diminished window of opportunity due to late delivery of software. Furthermore, the respondents overwhelmingly applied the treatment strategy of risk reduction to manage these risks. Additionally, these strategies were primarily project management processes, rather than technical processes. Therefore, this
demonstrates that project management is an RM strategy. In particular, managing stakeholders’ expectations is a specific risk treatment that helps to manage several key IT risks (Baccarini, 2004).

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

Conclusion

Risk is an integral component of IT projects, as well as to any projects. There are different types of risks and each depends on the kind of IT project involved. Risks can vary whether it is a software development project, or security project, or outsourcing project, or specific programming task. The role of RM was described in reference to several kinds of IT projects. The purpose of RM is to develop a detailed analysis of the project and to establish a comprehensive list of risks. RM assists project teams to make better decisions, communicate, and to resolve any risk issues in an effective matter. RM for IT projects described in the literature reviews share almost common steps.

This paper describes how important knowledge management is by providing an assessment for risk processes. This knowledge might result in enriching the repository with new information, modifying existing activities, identifying or retiring risks, and providing valuable feedback on the progress of the RM project. In order to have a deeper understanding of this theoretical framework and to answer the main research question, the integration of KM principles in support of RM processes, when applied to IT projects, may improve the organization’s ability to manage risks response planning by enhancing risk identification, analysis, and mitigation.

This paper tried to provide 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. The integration of KM and RM processes improve the reduction risk for IT projects. Implications will certainly help both academic researchers and practitioners to get a better understanding about the knowledge processes on risk management.

References


IRM. (2002), 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


