The Challenges in Implementing Risk Management for Information Technology Projects
Amine NEHARI TALET, Razali MAT-ZIN
KING FAHD UNIVERSITY OF PETROLEUM & MINERALS SAUDI ARABIA
Maaradj HOUARI
GHRADAIA UNIVERSITY ALGERIA

ABSTRACT

IT projects are characterized by high degrees of risk. The rapid speed of transformation in information technologies combines changes in business processes to create surprising shifts in cost, the cost benefit relationship, and the feasibility of doing specific things in particular ways. 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 the challenges experienced when executing risk management processes in information technology projects. The lack of knowledge management support for risk management processes has caused many project failures in the past.

KEYWORDS:: Risk Management (RM), IT projects, uncertainty, risk monitoring.

I. INTRODUCTION

The globalization of companies introduces many challenges. To meet these challenges, companies may require being innovative and introducing new ideas. The need to change is forcing corporations to organizing their projects and their system. Many companies depend on its own resources or external resources to meet their objectives and be better prepare for changes in their surrounding environment.

Moreover, corporations are facing new and different types of risks every day because of the changes in the world environment. These environments might introduce new or existing risks to the corporations. The source of risks differs from the internal or external environment. This risky environment if not managed appropriately might impact negatively on the existence and future corporations. For this reason managers have to take into consideration risks that can affect the organization and they have to minimize their impact on the organization.

IT projects are characterized by high degrees of risk. The rapid speed of transformation in information technologies combines changes in business processes to create surprising shifts in cost, the cost benefit relationship, and the feasibility of doing specific things in particular ways. The risks faced by IT projects are not, in essence, financial risks. By understanding these fundamental problems in real terms, rather than through their financial impact, IT project managers can move more quickly to resolve issues before they become major problems that threaten the goals of the project. Most IT practitioners understand that there are risks other than financial risk in projects.

IT project risk, includes 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).

II. LITERATURE REVIEW

1) Risk and Uncertainty

The well-known economist [1]founder of the Chicago School, distinguishes risk from uncertainty by relating risk to a “quantity susceptible of measurement” … “a measurable uncertainty” opposing it to real uncertainty “an unmeasurable one” This reference to measurable and quantifiable events is also found within the project management literature. [2]relate risk to an “identifiable event that will have negative
consequences whereas uncertainty relates to the source (of risk). [3]also define uncertainty as a situation being the source of risk: “a context for risks as events having a negative impact or opportunities that have beneficial impact. Extending the consequence of the identified event to opportunities has the commendable intention of encouraging the management of opportunities, but adds to the confusion when trying to distinguish risk from uncertainty. [4]have encouraged and largely influenced the use of the uncertainty concept over risk partly because the later is trapped in the perspective of negative perceptions of threatening events, which has the side effect of keeping practitioners from managing opportunities. A risk must contain two elements, namely uncertainty and loss [5]. RM refers to strategies, methods and supporting tools to identify, and control risk to an acceptable level [6].

2) Risk and Risk management

The present study does not investigate the concept of risk per se; it is focused more on “risk management” as a practice. Project risk management is related to the set of practices and tools generally used to manage project risk. Risks in an organization can extent the range of natural disasters, security breaches, and failings of human resource, third-part vendors, financial chaos, unstable business environments and project failures. Therefore, the different types of risks encountered in common organizations. Risk is the potential that a chosen action or activity (including the choice of inaction) will lead to a loss (an undesirable outcome). Risk is an uncertain event or condition that, if it occurs, has a positive or a negative effect on at least one project objective, such as time, cost, scope, or quality (where the project time objective is to deliver in accordance with the agreed-upon schedule; where the project cost objective is to deliver within the agreed-upon cost). A risk may have one or more causes and, if it occurs, one or more impacts. Also, risk conditions could include aspects of the project’s or organization’s environment that may contribute to project risk, such as poor project management practices, lack of integrated management systems, concurrent multiple projects, or dependency on external participants who cannot be controlled. Furthermore, risk refers to all events, incidences and actions that may prevent you or your organization realizing its ambitions, plans and goals. Risk is surrounding us in our personal and professional lives and it is a potential problem that might happen. However, regardless of the outcome, it’s a good idea to identify risk, assess its probability of occurrence and estimate its impact.

RM has the intent to take counter measures that either prevents risks or mitigates the impact of a risk. Several authors, including [7] argue that RM should form a primary part of the project management process. RM is a distinct discipline, which integrates knowledge from a variety of other business fields. It is the discipline in which a variety of methodologies are brought to bear on a specific problem. RM is very important and integral part of any business and well recognized by the project management institutions [8].

3) Risk Management

Most projects or business venture to take place in a changeable environment in which many drawbacks exist that might negatively impact the outcome of project success. A project is considered successful if it meets the requirements determined by the stakeholders, such as security, efficiency, reliability, maintainability, functionality, integration, and other requirements [7]. A study illustrated that 35% of deserted projects are not unnecessary until the implementation stage of the project [9]. This implies that project managers are doing a poor job of identifying or terminating projects that are likely to fail due to risks encountered during the project life cycle.

The concept of the risk management is applied in all aspects of business, including planning and project risk management, health and safety, and finance. It is also a very common term amongst those concerned with Information Technology. A generic definition of risk management is the assessment and mitigation of potential issues that are a threat to a business, whatever their source or origin. [10]
The concept is now fairly universally understood, having been in widespread use for a number of years. It is applied in all aspects of business.

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

Threat is the potential cause of an unwanted impact on a system or organization (ISO 13335-1). Threat can also be defined as an undesired event (intentional or unintentional) that may cause damage to the goods of the organization.

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

Risk management is a process consisting on:

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

RM is concerned with identifying risks, understanding risks and drawing up plans to minimize their effect on project. RM can be seen as a series of steps that help a software team to understand and manage uncertainty [11].

RM objective is to identify all applicable risks in a project or business or product. It involves ranking the above elements based on their importance, frequency of occurrence, level of impact and then establishes the actions needed to control the identified risks. It is possible for every individual risk aspect to be documented in further details [12]. 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.

The goal of performing risk management is to enable the organization to maintain at the highest values the activity results. This process should combine as efficient as possible, all factors which can increase the probability of success and decrease the uncertainty of achieving objectives. Risk management should be an evolving process. Particular attention should be given to the implementation of the strategies for eliminating or reduce the risk and their appliance, to the analysis of the past evolution of risks and to the present and future prediction of the events. Management process should be implemented at the highest management level.

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

4) Risk Management Process

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

- **Design the management system** involves identifying business requirements, assessing the likelihood and the impact of the risks, including the implementation of a security policy and selecting the adequate countermeasures for the existing risks;

- **Implement the management system** involves applying control measures and work procedures, resource allocation,
setting the responsibilities and conduct training and awareness programs;
- Monitoring, reviewing and reassessing the management system involve an evaluation of effectiveness of controls and working procedures, of business changes, of previous incident reports and of existent risks;
- The improvement and update of the management system involves correcting the identified dysfunctions, or eliminating the unsustainable decisions or applying new control measures.

Risk management encompasses three processes: risk assessment, risk mitigation and the reassessment of the residual risk.

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

<table>
<thead>
<tr>
<th>Table 1: The processes of RM have appeared in a number of existing process models in the area of RM</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>References</th>
<th>Description of Process</th>
</tr>
</thead>
<tbody>
<tr>
<td>13</td>
<td>Risk monitoring Risk control planning Risk analysis Risk identification Software development process</td>
</tr>
<tr>
<td>14</td>
<td>Risk Control Risk Track Risk Plan Risk Analyze Risk Identification Software risk management</td>
</tr>
<tr>
<td>15</td>
<td>Risk Monitoring Risk Control Risk Analysis Risk Control Planning Risk Identification Review Define Goals Role in software engineering</td>
</tr>
<tr>
<td>16</td>
<td>Risk Control Risk Tracking Risk Planning Risk Analysis Risk Identification RM as verification and validation</td>
</tr>
<tr>
<td>17</td>
<td>Risk Prioritization Risk Analysis Risk Identification Software project management</td>
</tr>
<tr>
<td>11</td>
<td>Risk monitoring Risk analysis Risk Identification Software development</td>
</tr>
<tr>
<td>6</td>
<td>Risk Control Risk Tracking Risk Planning Risk Analysis Risk Identification Great definition review Data warehouse system</td>
</tr>
<tr>
<td>10</td>
<td>Risk Monitoring Risk Evaluation Risk Evaluation Risk Identification RM in insurance field</td>
</tr>
<tr>
<td>19</td>
<td>Resolve Risks Prioritize and map risk Analyze Risks Identify Risks Controlling product development</td>
</tr>
<tr>
<td>20</td>
<td>Risk monitoring and control Risk response planing Quantitative risk analysis Qualitative risk analysis RM planning Project management</td>
</tr>
<tr>
<td>21</td>
<td>Risk Monitoring Risk Planning Risk Analysis Risk Identification Software engineering</td>
</tr>
<tr>
<td>22</td>
<td>Evaluate RM process Perform risk treatment Perform risk monitoring Perform risk analysis Manage the project risk profile Plan and implement risk management Software Risk Management Process</td>
</tr>
<tr>
<td>23</td>
<td>Risk monitoring Risk mitigation Initial risk assessment Risk identification Risk classification Risk architecture</td>
</tr>
</tbody>
</table>
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 never entirely eliminate the risks.

RM process is divided into Risk Identification, which results in a variety of technological content, environmental communication and operation approaches, programmatic constraints and the mission duration[16]. 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. 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.

RM process is described into six steps: 
1) Goal Definition: review the stated goals for the project, refine them and define implicit goals and constraints explicitly.
2) Identification: identify potential threats to the project using multiple approaches.
3) Analysis: classify risks, complete risk scenarios, estimate risk effects and estimate probabilities and utility losses for risk scenarios.
4) Control and Planning: select the most important risks, propose controlling actions and the actions for implementation.
5) Control: implement the risk controlling actions. 6) Monitoring: monitor the risk situation [15].

Figure 1 illustrates the proposed Riskit method by [15].

RM process contains the following processes: identifying risks using brainstorming techniques to discover any risks that prevent the progress of the project, analyzing risks by the team members to determine if a certain risk is worth migrating or not, prioritizing and mapping risk to establish a seriousness of the risk according to their impact, and resolving risks by implementing plans to prevent risk from occurring [24].

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 2 illustrates the RM process[25].
Figure 2: RM Processes [25]

5) Sources of Risks in IT projects

By examining the literature reviews, IT projects can range from software development, outsourcing, communications and implementing a new security infrastructure. Also, these IT project risks might have a particular management in a different project. Risks are resulting of many factors involved in the projects. Each factor will depend on the type and purpose of the project IT projects are characterized by high degrees of risk. The rapid pace of change in technologies combines changes in business processes to create unpredictable shifts in cost, the cost benefit relationship, and the feasibility of doing specific things in particular ways [26].

One classic problem identified in many IT projects occurs when new technologies are developed as the project is underway [27]. 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 [28]. 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.

[29] break IT project risk 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).

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 [30]. However, many more projects continue long after any hope of success has faded ([31]; [32]).

IT projects are much more likely to fail than other types of projects, such as building construction projects and states that the main causes for IT project failures are their use of rapidly changing technologies, their generally long development times, and the volatility of user expectations about what the project will yield. Because IT projects generally include all of these characteristics, they are prone to failure, cost overruns, and schedule delays [33].

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 [34].

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

1. IT projects are known for their high failure rate. Based on 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 [35]. 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 a RM strategy. In particular, managing stakeholders’ expectations is a specific
risk treatment that helps to manage several key IT risks[35]. The risk issues in reference to software development process were not viewed as essential subject of discussion. On the other hand, most organizations hope to implement systems successfully while still assuming their regular business processes. Yet, new systems are not implemented in a space and many authors concur that the first step in developing a business continuation plan is to carry out a risk assessment. Examples of risks associated with software development are[36]

III. CONCLUSION
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. In the last section, a description of RM framework describing the processes developed by different authors for IT projects. The purpose of RM is to develop a detail analysis of the project and to establish a comprehensive list of risks. RM assists project team to make better decisions, communication and to resolve any risk issues in effective matter. RM for IT projects described in the literature reviews share almost common steps.

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

BIBLIOGRAPHY
17. J., Jurison, "Software projectmanagement: The manager’s view.," Communications of


http://www.projectsmart.co.uk/pdf/pmbok.pdf


