

A Risk Management Model for Project Execution

Samer ALHawari, the Arab Academy for Banking and Financial Sciences, Amman-Jordan,
Samer.alhawari@yahoo.com

Fadi Thabtah, MIS Dept, Philadelphia University, Amman, Jordan
Ffayez@philadelphia.edu.jo

Louay Karadsheh, Lawrence Technology University, Southfield, MI, USA,
louay.karadsheh@gmail.com

Wa'el Musa Hadi, the Arab Academy for Banking and Financial Sciences, Amman Jordan,
Whadi1981@yahoo.com

Abstract

Risk management is becoming a key factor within organizations since it ensures a successful execution of projects. In an organization life cycle, there is simply no way to guarantee a completely risk free workplace. Moreover, information is essential to efficient and effective business processes and it is a critical success factor for a competitive market position. Due to this fact, information flows and process structure must be managed carefully to reduce risks that might face the progress of projects. This research aims to present a conceptual framework of the risk management process cycle. An articulate model of risk is developed based on a thorough analysis of various models presented in the literature. The main emphasis is on developing phases such as scrutiny, verifying, planning of experiments, and risk education across the risk management process cycle. This should improve the implementation of risk management processes.

Key Words: Risk, Risk management, Risk management process model, Risk analysis.

1. Introduction

Risk management is concerned with identifying risks; understand risks and drawing up plans to minimize their effect on project. Risk management can be seen as a series of steps that help a software team to understand and manage uncertainty [1]. Risk refers to all events, occurrences 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 the outcome, it's a good idea to identify risk, assess its probability of occurrence, and estimate its impact. The reasons for studying risk management 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. Risk management is a distinct discipline, which integrates knowledge from a variety

of other business fields. It is discipline in which a variety of methodologies are brought to bear on a specific problem. Risk management is very important and integral part of any business and well recognized by the project management institutions [8].

1.1 Risk and Risk Management

Most projects or business ventures 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, etc. ([17], [15]) contend that the high failure rate of projects is in fact due to not taking preemptive actions to evaluate and handle risks involved. A study by [9] illustrated that 35% of deserted projects are not discarded until the implementation stage of the project. 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.

There are several definitions of risk, such as the likelihood that an organization will be negatively affected during the process of acquiring, deploying and using information technology. [16] Describes risk as any variable in the project that causes project failure. A risk must contain two elements, namely uncertainty and loss [16]. Risk management refers to strategies, methods and supporting tools to identify, and control risk to an acceptable level [4]. Risk management has the intent to take counter measures that either thwart risks or mitigate the impact of a risk. Several authors, including [17] argue that risk management should form a primary part of the project management process. [14] Recommend that the list of potentially recognized and appropriate risks should be incorporated in all project plans or business processes.

Risk management 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 [7]. Since no one can predict what losses will occur, the objective of risk management is to ensure that no risk will occur during the execution of project in order to minimize losses to an acceptable level. If a loss occurs, then the objective of risk management has failed to achieve the objectives intended, which prevent the organization from pursuing their goals.

The rest of the paper is structured as follows: Section 2 reports the existing theories on the risk management process, Section 3 proposes a new risk model which improves the activities in existing risk model cycles, leading to more reliable information to support management decisions. Finally, we conclude the paper in Section 4.

2. Literature Review

This section gives the readers an overview of the different research contributions in risk management literature. There is several different risk management processes used in organizations today, these are summarized in Table 1. The processes of risk management have appeared in a number of existing process models in the area of risk management.

Table 1: Risk management process

Main Dimension/ Risk Management Process	Sub Dimension/ Description of Process							References
	1	2	3	4	5	6	7	
Risk Management Process	Risk Identification	Risk Evaluation	Risk Control	Risk Monitoring				[2] (Beck et al., 2002)
Risk Management Process	Risk Identification	Risk Analysis	Risk Planning	Risk Tracking	Risk Control			[5] (Cornford, 1998)
Risk Management Process	Review define goals	Identify and monitor	Analysis Risk	Plan risk control	Control Risk			[12] (Kontio, 1996)
Risk Management Process	Risk management mandate definition	Goal Review	Risk Identification	Risk Analysis	Risk control planning	Risk control	Monitor Risks	[3] (Boehm and Bose, 1994)
Risk Management Process	Risk Identification	Risk Analysis	Risk Prioritization					[11] (Jurison, 1999)
Risk Management Process	Identify Risks	Analyze Risks	Prioritize and map risk	Resolve risks	Monitor Risks			[18] (Smith and Merritt, 2002)
Risk Management Process	Risk Identification	Risk Analysis	Risk Planning	Risk Monitoring				[19] (Sommerville 2001)
Risk Management Process	Risk Identification	Risk analysis	Risk monitoring					[1] (Bandyopadhyay et al 1999)
Risk Management Process	Goal definition review	Risk Identification	Risk Analysis	Risk Planning	Risk Tracking	Risk Control		[4] (Bruckner et al 2001)
Risk Management Process	Risk Identification	Risk Analyze	Risk Plan	Risk Track	Risk Control	Risk Communication		[10] (Higuera and Haimes 1996)

[2] Divided risk management into four phases. The first phase 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 phase is risk evaluation, which is producing a list of all possible threats to the e-business in relation to the likelihood and their severity. The third phase 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 phase 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.

A structure designed by [5] described risk management process into risk identification which results in variety of technological content, environmental communications, the execution and operation approaches, programmatic constraints and the mission duration. 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 phase 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 different 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.

[12] Described risks as reviews that define the goals and objective, identify and monitor potential risk, which includes a prioritized quantified risk, and plan risk control. [3] Provided a comprehension definition of risk as the scope and frequency of risk management. He divided risk management into four phases. Firstly, the risk identification, which is used to locate potential threats, secondly, the risk analysis which is used to classify and consolidate risks. Thirdly, the risk control planning, which is targeted to select the most important risks to control planning, and lastly, the risk

monitoring, which is utilized to observe the situation of risks.

A framework proposed by [11] described the risk assessment in three steps; the first one is risk identification, which is purposed to develop a list of risks that can adversely impact project outcome. The second step is risk analysis, which is intended to assess the risk exposure, the likelihood and impact of each risk and the final step is the risk prioritization, which is used to produce a list of risks prioritized by the impact.

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

[19] Stated that risk management involves the following stages: 1) Risk identification 2) Risk analysis 3) Risk planning 4) Risk monitoring. [1] acknowledged that the risk management process involves 1) Risk identification, which entails checklist, questionnaires or brainstorming meeting 2) Risk analysis to assess the identified risk in order to create a contingency measures to decrease the risk impact and 3) Risk monitoring to guarantee the effectiveness of the methods followed.

A research done by [4] suggested that risk management process should contain 1) Goal identification phase to define project objectives and stakeholders 2) Risk identification phase to identify all relevant risks 3) Risk analysis phase, which contains several steps such as risk probability, risk impact and risk exposure 4) Risk planning phase, which contains risk contingency strategy, risk tracking and risk control.

A model by [10] described risk management process in six steps starting with identification phase to recognize all risks, analysis phase to convert risk data in to appropriate information, plan phase to convert the risk information into actions, track phase to monitor the risk status and actions taken to mitigate the identified risks, control phase to correct any divergence from their planned actions, and finally the risk communication phase to stress the occurrence and its importance.

3. The Proposed Risk Management Framework

This section proposes a risk management framework see (Figure 1), which contains some key elements, namely the need for risk management, goal definition review, identify risk, risk scrutiny, risk analysis, risk verification, planning for risk, planning experiment ,risk implementation ,risk control , risk monitoring and risk education. These elements are fully discussed in this section.

3.1 The Need for Risk Management

In this conceptual framework, the first element is the need for risk management which addresses the necessity for the organization to implement risk management processes. The organization must explicitly define the importance of risk management to

their stakeholders to contribute in identifying all risks associated with business objectives. Identifying all relevant stakeholders is essential for the success of the risk mitigation process [13]. These risks may be obstacles for the organization in achieving the stated business objectives. When an organization plans a new business strategy, it must identify all risks associated with it in order to mitigate the obstacles and to facilitate the implementation of the new strategy in terms of the goals. Risk management is needed in day-to-day business operations and project management implementation. Understanding the need of the risk management is vital for success of organization existence in dynamic world. The need will establish the goal definition for implementing the risk management.

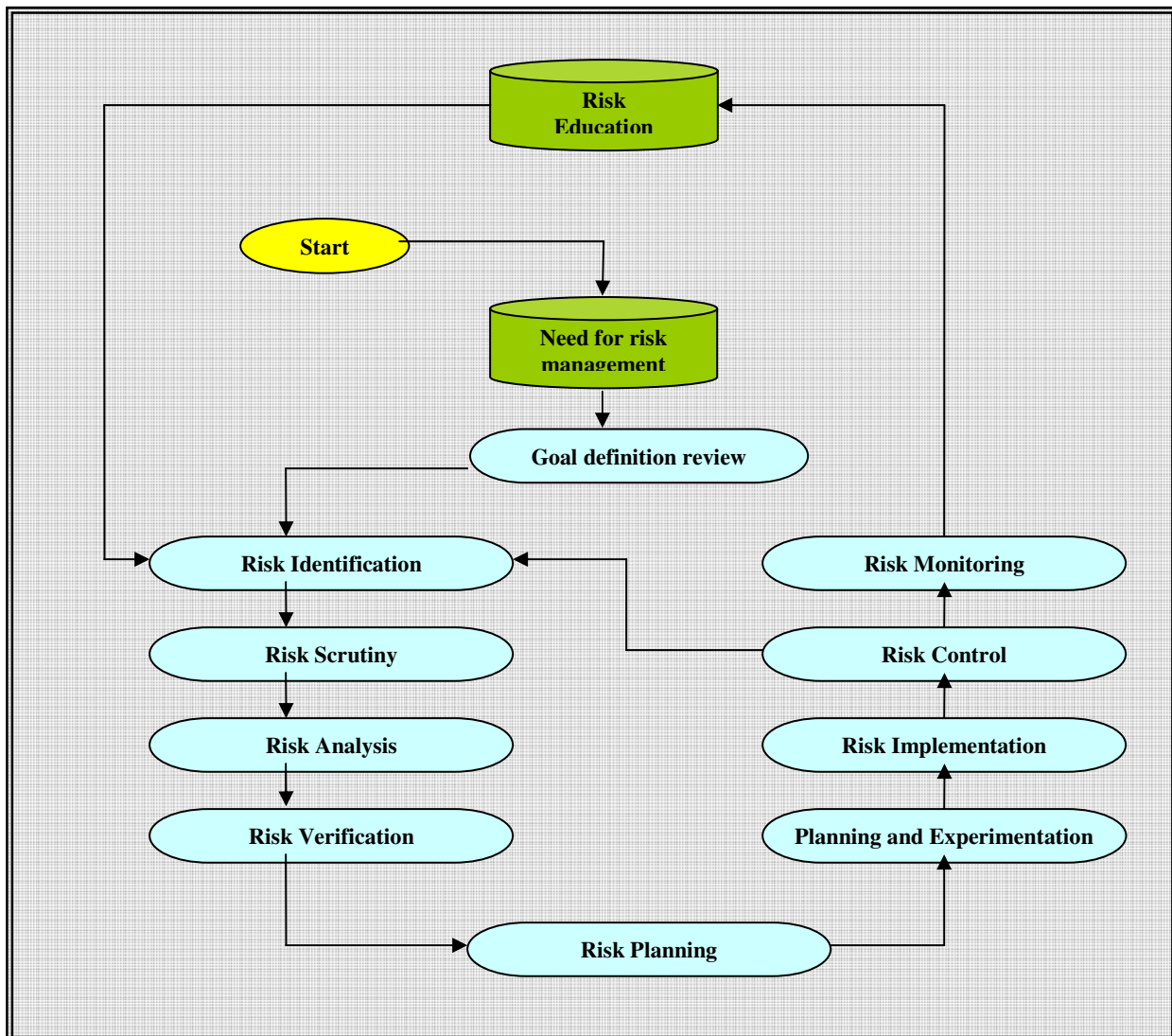


Figure 1: Conceptual Framework for Risk Management

3.2 Goal Definition Review

During the goal definition review, the organization mission and vision is defined. The goal definition states the organization goals, clearly defines the constraints and implicit goals and analyzes the goals of the stakeholders [13]. The next step in this phase is to define the strategy, [12] describes the importance of reviewing and defining the goals in order to clearly output the objectives, expectation and constraints.

3.3 Risk Identification

This element of our framework is concerned about risks associated with project's objectives. Managing risk requires risk identification, which helps in surfacing risk before it becomes a [10]. According to [4], risk identification should include the grounds of the risk and its predictable result if that risk occurred. This phase requires comprehension recognition of all threats to the business projects. This phase should also produce a list of all risks associated with any project [11]. The sources of risk can come from technology content, environment contact, execution and operations, constraints, etc [6]. The risk identification phase must be repeatedly implemented through out the project life cycle, and should classify the risk as high, medium or low, where this classification mainly depends on the organization security policy. A checklist, questionnaires or brainstorming sessions are vital techniques in this phase [16] as well as interviewing key stakeholders, auditing reports and customer complaints are valuable practices. The final output of the risk identification is a list of all possible risks.

3.4 Risk Scrutiny

It concentrates on evaluating every potential listed risk from the previous stage that might face the organization. The evaluation of every risk is based on the organization objectives. The purpose of this phase is to profoundly study every risk that might occur, then to eliminate any risk that is not associated with or has no impact on the project progress. This phase will add to the list, the likelihood of occurrence for every risk [2], which should provide a better view of the risks in order to correctly analyze them in the next phase. The output of this phase is the relevant risks with their likelihood of occurrences.

3.5 Risk Analysis

This element facilitates the conversion of risk data into decision making information [10]. This phase can be divided into risk probability which 1) describes the likelihood of event 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. [4] Averted that a high-probability

risk might have a low impact and a high impact risk might have a low probability and both can be ignored safely. On the other hand, a high probability with high impact risk should be managed immediately. Risk analysis can provide an estimate of the impact of the risk either quantitatively or qualitatively depending on the method used. This phase facilitates the prioritizing of the risks according to the project objectives. [3] Described risk analysis phase through conducting scenarios for major risks, and events. These results in estimates of risk effects for all the conducted cases described in the scenarios and establish a probability of losses for every risk scenario. The output of the risk analysis phase is a detailed description of every valid risk, severity, impact, priority, probability and impact estimates. This phase 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.

3.6 Risk Verification

It reviews the risk analysis output in order to determine whether the listed risks are relevant to the organization goals and could formulate real threats. This phase must be conducted by different employees in the organization who are not associated with the team who worked on the previous phase. The purpose of this phase is to filter out all risks not relevant to the organization goals and objectives. The filtering technique provides useful resources for the real risk pretending to business objectives, and saves the organization resources from working on risks not related to their goals.

3.7 Risk Planning

It assists in converting the risk information into action and judgment and involves developing actions to deal with each risk, prioritizing measures, and creating a management plan [10]. 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 [4]. The planning phase recommends the risk controlling actions needed in the later stages and requires selecting the proper security control methods according to the impact and the likelihood of risks. This phase also provides different execution possibilities and examines different "What-if" options. The phase outputs according to [2] are simple rules, process controls, testing, modeling and inheritance.

3.8 Planning and Experimentation

It tests whether the risk planning performed in the previous step is accurate and comprehensive. This phase also checks whether all risks are applicable to

the organization and are correctly classified according to their impact and likelihood. This phase main goal is to prevent wasting resources during the implementation phase by assuring the validity of the risk using techniques such as structured walk-through, checklist, simulation, etc.

3.9 Risk Implementation

It is the phase, the activities in the planning stage are executed and security controls are implemented according to plans formulated in the previous stages. An important part of this phase is to define the timeframe and the team members' responsibilities. This phase also requires a strict controlling procedure during the implementation process. There are different implemented measures, which can be considered in order to deal with risks such as risk avoidance, risk reduction, risk transfer, etc [2].

3.10 Risk Control

This is the evaluation phase of the implementation process and its mainly used to discover new risks. The risk control phase is an update process for the whole risk management life cycle, which produces report of the execution progress of the risk cycle to ensure the sufficiency of the alleviation approach.

3.11 Risk Monitoring

It consists of observing the risk status and actions, and it provides a real-time monitoring to modify the risk execution process in order to maintain an update risk lists [6]. Risk monitoring is vital to effective implementation of action plans. The organization exists in a changing environment which might introduce a new risks never been known before. Also organization might introduce a new system which requires a reassessment resulting in an updated risk plan. [8] Stated that risk monitoring must deal with risk evolution such as factors, triggers and responses, which might result in going back to previous stages for modification or updating. Risk monitoring phase is an effective tool for controlling the risk management execution cycle [6].

3.12 Education

It is the final stage in the risk management cycle, where all experiences captured during the previous cycles are stored in a repository. It might be lessons learned to provide useful instructions for future encountered situations that closely match a previous experience. This final stage helps individuals utilizing the knowledge possessed by other individuals without attaining the knowledge. Risk education is aimed on providing a list of previous encountered risk for similar case or project which can shorten the risk identification timeframe process.

4. Conclusions

This paper presents a conceptual framework of risk management process. The objectives of this paper is to describe a more valid process to identify how organization deals with risk management, and presents a robust risk management life cycle with extensive and detailed processes. Based on the topic of this research, this paper concluded that the proposed risk management model would give a broadest analysis of the risk management process. To the best of the author's knowledge, there are few risk management models in the literature, which includes phases such as scrutiny, verification, planning experiment, and risk education. These phases which the proposed model considers improve the implementation process.

References

- [1] Bandyopadhyay, K., Myktyyn, P.P., and Myktyyn, K. "A framework for integrated risk management in information technology," *Management Decision* (37:5), 1999, pp. 437-444.
- [2] Beck, M., Drennan, L., and Higgins, A. "Managing E-Risk," *Published by London: the Association of British Insurers*, 2003, ISBN: 10903193-23-0, Obtainable on: www.abi.org.uk.
- [3] Boehm, B.W., and Bose, P.A. "Collaborative Spiral Software Process Model Based on Theory," *Proceedings of the third International Conference on the Software Process*, 1994, IEEE Computer Society, Washington, DC.
- [4] Bruckner, R.M., List, B., and J. Schiefer, J. "Risk-Management for Data Warehouse Systems," *Lecture Notes in Computer Science* (2114), 2001, pp. 219-229.
- [5] Cornford, S. "Managing Risk as a Resource using the Defect Detection and Prevention process," *International Conference on Probabilistic Safety Assessment and Management*, 1998, pp.13-18.
- [6] Cornford, S., Feather, M., and Hicks, K. "DDP-Tool for life-Cycle Risk Management. Jet Propulsion Laboratory," *California Institute of Technology*, 2001, IEEE.
- [7] Cule, P., Schmidt, R., Lyytinen, K., and Keil, M. "Strategies for Leading off is Project Failure." *Information Systems Management*, spring, (17:2), 2000, pp. 65-73.
- [8] Del Cano, A.D., and de la Cruz, M.P. "Integrated Methodology for Project Risk Management." *Journal of Construction Engineering and Management*, (128:6), 2002, pp. 473-485.

- [9] Ewusi-Mensah, K., and Przasnyski, Z.H, "On Information Systems Project Abandonment: An Exploratory Study of Organizational Practice," *MIS Quarterly*, (15:1), 1991, 67-88.
- [10] Higuera, R.P., Haimes, Y.Y. "software risk management," *Technical Report (CMU/SEI-96-TR-012 ESC-TR-96-012) Pittsburgh, Pa.: Software Engineering Institute*, 1996, Carnegie Mellon University.
- [11] Jurison, J. "Software Project Management: A Manager's View, " *Communications of AIS* (2:17), 1999.
- [12] Kontio, J. "The Riskit Method for Software Risk Management, *version 1, 00*," CS-TR-3782 / UMIACS-TR- 97-38, 1997, *Computer Science Technical Reports*. University of Maryland. College Park, MD.
- [13] Kontio, J., Getto, G., and Landes, D. "Experiences in improving Risk Management Processes using the concepts of the Riskit Method," *In Proceedings of the ACM SIGSOFT 6th international symposium on Foundations of software engineering ACM Press*, New York, 1998, pp.163-174.
- [14] Lubelczyk, J., and Parra. "A Recommended Approach to Software Development," *Revision 3. Software Engineering Laboratory*, NASA.1992.
- [15] May, L.J. "Major Causes of Software Project Failures," 1998, Available at: <http://stsc.hill.af.mil/crosstalk/1998/jul/causes.asp>. Accessed, April, 2007.
- [16] Padayachee, K. "An Interpretive Study of Software Risk Management Perspectives," *Proceedings of SAICSIT*, 2002, pp.118-127.
- [17] Powell, P.L., and Klein, J.H. "Risk Management for Information Systems Development," *Journal of Information Technology* (11), 1996, pp.309-319.
- [18] Smith, P.G., and Merritt, G.M. "Proactive Risk Management: Controlling Uncertainty in product Development, " 2002, New York: productivity press.
- [19] Sommerville, I. *Software Engineering*, 6(Edition), 2001, pp. 84-85.