A DEA-Based Approach for Information Technology Risk Assessment through Risk Information Technology Framework

Morteza Hatefi[1] and Mehdi Fasanghari[2]
[1]Faculty of Engineering, Shahrekord University, Iran
[2]Cyber Space Research Institute, North Karegar St, Iran

Abstract: *The use of Information Technology (IT) in organizations is subject to various kinds of potential risks. Risk management is a key component of project management enables an organization to accomplish its mission(s). However, IT projects have often been found to be complex and risky to implement in organizations. The organizational relevance and risk of IT projects make it important for organizations to focus on ways in order to successfully implement IT projects. This paper focuses on the IT risk management, especially the risk assessment model and proposes a process oriented approach to risk management. To do this end, this paper applies the risk IT framework which has three main domains, i.e., Risk Governance (RG), risk analysis, Risk Response (RR) and 9 key processes. Then, a set of scenarios, which can improve the maturity level of risk IT processes, are considered and the impact of each scenario on the risk IT processes is determined by the expert opinions. Finally, the Data Envelopment Analysis (DEA) is customized to evaluate improvement scenarios and select the best one. The proposed methodology is applied to the Iran Telecommunication Research Centre (ITRC) to improve the maturity level of its IT risk management processes.*

Keywords: *Risk IT framework, risk management, process model, DEA.*

Received June 10, 2012; accepted September 14, 2013; published online December 3, 2014

1. Introduction

Implementing Information Technology (IT) projects provides appropriate and useful information to support operation, management analysis, and decision making through the enterprise [42, 45]. Risk is an entity that appears in all aspects of a project and always will have a negative impact. Consequently, the need for project risk management has been broadly recognized. Integration of risk management into some business-related issues such as business process modelling, e-commerce environment, and agreement networks can be traced in [30, 34, 35]. Project risk management improves the project performance by systematically identifying and assessing risks, developing policies to reduce or avoid them and maximizing opportunities [6]. IT risk is a relatively new term, which relies to the consequences of adverse events arisen from IT. Two well-known methodologies have been introduced to cope with this type of risk, i.e., enterprise risk management and Information Systems Audit and Control Association (ISACA's) risk IT frameworks that are the most recent ones in the literature [3, 8, 15, 22, 39].

Risk identification, Risk Evaluation (RE) and Risk Response (RR) are the main steps in risk management [9]. There are various frameworks and approaches used in the literature for risk managements of projects. Among them, we can refer to Tummala *et al.* [40] that proposed a methodology for risk management, in which several steps are considered, i.e., identifying, measuring, evaluating risk, risk control and monitoring.

Benaroach *et al.* [5] applied the option-based risk management framework to control risk and maximize value in IT investment decisions. The authors developed risk management plans for a broad portfolio of 50 investments and found empirical support for risk option mappings. Alhawari *et al*. [1] proposed a conceptual framework for managing risks based on the Knowledge Management (KM), which employs KM processes to improve its effectiveness and increase the probability of success in innovative IT projects. Furthermore, Huang *et al*. [18] introduced a two-level model for risk management of virtual enterprise. The authors resort to the distributed decision-making to describe the decision processes of the owner and the partners. Mathrani and Mathrani [29] investigated that how enterprise system data was transformed into knowledge and how these knowledge was used to manage enterprise risks by using a data transformation model. A decent literature review on project risk management is provided by Williams [44]. A wide range of risk analysis tools and techniques are presented and classified by the author and finally managerial insights are provided for managing risks. This paper uses the risk IT framework which is a novel and comprehensive framework for managing the risks of IT projects. The risk IT framework is part of the ISACA product portfolio on IT governance. According

to the risk IT framework [22], Risk Governance (RG), RE and RR are the main domains for managing IT risks. The main advantage of the risk IT framework over other existing risk management frameworks is that it focuses on the RG domain, which contains three key processes, i.e., establishing and maintaining a common risk view, integrating with enterprise risk management and making risk-aware business decisions. However, this domain and its processes are not clearly reflected in the risk management frameworks introduced in the literature.

A wide range of tools, techniques and structured models have been proposed for RE and assessment in the literature. Multi criteria decision making tools are widely used to develop risk assessment models. For instance, Karimi *et al*. [24] develop a systematic procedure based on fuzzy TOPSIS concepts for selecting the best risk assessment model by considering several criteria. Mustafa *et al.* [10, 31] tackle an Analytic Hierarchy Process (AHP) and a multiple attribute decision-making technique to cope with risk analysis of construction projects with the involvement of the related stakeholders. Lo and Chen [28] proposed a hybrid procedure that evaluates risk levels of information security under various security controls. A RE method for a high-tech project investment is proposed by Liu *et al.* [26]. The authors constructed an evaluation indicators system and then introduced the evaluation procedure based on an uncertain linguistic weighted operator. Hongxia and Baihua [16] proposed an IT project risk assessment model based on a fuzzy AHP approach. Othman [32] constructed an evaluation index system with five risk factors to prevent communication accident and improve project management ability. Then, the author applied the method of fuzzy comprehensive evaluation to assess the overall risk for a core network expansion project in Xinjiang telecommunication. Yucel *et al.* [46] proposed a fuzzy risk assessment model based on the analytic network process and fuzzy inference system for implementing information system in hospitals. This paper employs the data envelopment analysis, which is a powerful and optimisation based tool in decision making process. Fortunately, Data Envelopment Analysis (DEA) is an effective and applicable tool to derive weights from the view point of operation research. DEA is capable to perform weighting and aggregating steps simultaneously and does not need to expert opinion and analyst judgment to do so.

Although, there are several studies focused on risk management in the conventional projects, there is a rare literature on risk management in IT projects [37, 38]. Additionally, most of the existing studies are not comprehensive and just focus on a specific type of risks [4]. Among them, we can refer to the works presented in [19, 33, 41]. A framework is developed by Vitale [41] to identify the strategic IT-related risks. Rainer *et al.* [33] cope with the IT risk analysis by integrating qualitative and quantitative methodologies. Huang *et al.* [19] develop a risk prioritizing methodology in ERP projects based on analytic hierarchy process. Their methodology considers both qualitative and quantitative factors and involvement of the concerned stakeholders. An international Delphi study is performed by Schmidt *et al.* [36] to identify software project risks.

The objective of IT risk management is to protect IT assets such as data, hardware, software, personnel and facilities from all external threats (e.g., natural disasters) and internal threats (e.g., technical failures, sabotage, unauthorized access) so that the costs of losses resulting from the realization of such threats are minimized. A large body of the literature of IT risk management are assigned to the software project risk management [23, 47]. In this line of research, we can refer to Li *et al*. [25, 43], which consider the risk factors during developing software projects. Baccarini *et al.* [3] recognized and ranked IT project risks and proposed possible response strategies. However, the authors did not provide any framework for software risk management. Besides, Guiling and Xiaojuan [12] provide a research on the risk management of IT software projects.

The aim of this paper is to evaluate a set of scenarios and select the best one whereby the maturity of IT governance may be increased from the IT risk management point of view. To do this end, a DEA-based approach is proposed to assess the scenarios based on the risk management processes introduced in the risk IT framework. DEA, introduced by Charnes *et al.* [7] is a powerful decision making tool that is widely used for productivity and efficiency analysis. Various extensions and applications of DEA models can be traced in the literature [8, 13, 17]. To the best of our knowledge, this study is the first one that resorts to DEA concepts for risk management in IT project.

The rest of the paper is organized as follows: Section 2 briefly presents two classical DEA models for evaluating and ranking decision making units. Section 3 provides a brief explanation of the risk IT framework introduced by ISACA [22] and its processes. The proposed approach is elaborated in section 4. In section 5, the proposed approach is applied on ITRC to improve its risk management processes. Related results are presented in this section. Finally, concluding remarks are discussed in section 6.

2. Data Envelopment Analysis

DEA is a mathematical programing model tackles the problem of measuring the performance of a set of homogeneous Decision Making Units (DMUs) [7]. Suppose there are n DMUs that uses m inputs (x_{ij}, i= 1, 2, ..., m) to produce s outputs (y_{ij}, r= 1, 2, ..., s). The standard DEA model assesses the efficiency of a

specific DMU (DMU_k) by maximizing the ratio of its weighted sum of outputs to its weighted sum of inputs with the condition that this ratio should not exceed one for all DMUs. The fractional DEA model developed Charnes *et al*. [7] is written as follows:

$$\begin{aligned} Max\ \theta_k &= \frac{\sum_{r=1}^{s} u_r y_{rk}}{\sum_{i=1}^{m} v_i x_{ik}} \\ s.t.\ & \frac{\sum_{r=1}^{s} u_r y_{rj}}{\sum_{i=1}^{m} v_i x_{ij}} \le 1,\ \ j=1,2,....,n \\ & v_i, u_r \ge \varepsilon > 0\ for\ all\ i, r \end{aligned} \tag{1}$$

Where v_i and u_r denote the weights assigned to the input i and output r, respectively. In addition, epsilon ε is a non-Archimedean infinitesimal value and θ_k denotes the performance score of DMU_k when it is under evaluation. Multi Criteria Decision Analysis (MCDA) and DEA are two popular methods for weighting and aggregating criteria in decision making problems. The weights are exogenously assigned to the criteria in many MCDA methods. However, assigning appropriate weights to criteria is a major problem when applying MCDA methods. Moreover, expert opinion and analyst judgment can have a significant impact on assigned criteria weights and consequently, affect the quality of final efficiency score [14]. Fortunately, DEA performs weighting and aggregating steps simultaneously and does not require any subjective and exogenous expert opinion and analyst judgment. The weights of criteria are endogenously and iteratively generated by DEA models.

The linear fractional programming Equation 1 can be converted to a linear programing model as follows [7]:

$$\begin{aligned} Max\ \theta_k &= \sum_{r=1}^{s} u_r y_{rk} \\ s.t.\ & \sum_{i=1}^{m} v_i x_{ik} = 1, \\ & \sum_{r=1}^{s} u_r y_{rj} - \sum_{i=1}^{m} v_i x_{ij} \le 0,\ \ j=1,2,....,n \\ & v_i, u_r \ge \varepsilon > 0\ for\ all\ i, r \end{aligned} \tag{2}$$

Equation 2 is an input-oriented DEA model with m inputs and s outputs for all the DMUs. The goal of input-oriented DEA Equation 2 is to maximize the outputs while keeping the inputs at their current levels. Notably, the efficiency of all DMUs is provided by solving Equation 2 repeatedly for each DMU. The efficiency of k^{th} DMU (θ_k) is between zero and one.

The k^{th} DMU is efficient if it achieves an efficiency score of one and it is inefficient if it receives an efficiency score smaller than one.

In the aforementioned models, it is assumed that inputs and outputs are explicitly defined for performance evaluation. However, there are many real cases that data are used without inputs (such as index data or pure output data). Liu *et al.* [27] developed a wide range of DEA models without explicit inputs and called them as DEA-WEI models. This type of models is applicable to the case where inputs are not directly considered. The DEA-WEI for Equation 2 can be written as follows [27]:

$$\begin{aligned} Max\ \theta_k &= \sum_{r=1}^{s} u_r y_{rk} \\ s.t.\ & \sum_{r=1}^{s} u_r y_{rj} \le 1,\ \ j=1,2,....,n \\ & u_r \ge \varepsilon > 0\ for\ all\ r \end{aligned} \tag{3}$$

In Equation 3, it is assumed that all performance measures are outputs. Equation 3 is equivalent to an input-oriented CRS DEA model with s outputs and one dummy input of 1 for all DMUs [14].

Sometimes, standard DEA models produce several efficient DMUs, i.e., DMUs with the efficiency score of 1 and therefore, fail in discriminating efficient DMUs and determining the best DMU. In order to, rank the efficient DMUs, Anderson and Peterson [2] propose a DEA model (hereafter AP-model) that permits the efficient DMUs to achieve a score greater than 1 by eliminating the constraint that bounds the efficiency score of k^{th} DMU, when evaluating this DMU. It is worth pointing out that the efficiency score greater than 1 does not any means. It just applies to rank efficient DUMs. The AP-model without explicit inputs (hereafter AP DEA-WEI model) will be formulated as follows:

$$\begin{aligned} Max\ \theta_k &= \sum_{r=1}^{s} u_r y_{rk} \\ s.t.\ & \sum_{r=1}^{s} u_r y_{rj} \le 1,\ \ j=1,2,....,n,\ j \ne k \\ & u_r \ge \varepsilon > 0\ for\ all\ r \end{aligned} \tag{4}$$

3. Risk IT Framework

Recently, ISACA introduces a comprehensive framework for managing IT risks, which complements ISACAs COBIT for control and governance of IT-based solutions and services [22]. The risk IT, Val IT and COBIT are three well-known and interrelated frameworks that are developed by ISACA to manage risk, value and IT-related processes within the enterprise respectively [20, 21]. Among these frameworks, IT risk framework is professionally focused on managing IT risks. The risk IT framework is constructed based on the set of principles that are aligned with the methods and the processes of Enterprise Risk Management (ERM). On the other words, effective enterprise governance of IT risks always aligns IT objectives with business objectives, aligns the IT risk management with ERM, balances the costs and benefits of IT risk management, promotes fair and open communication of IT risks, establishes the right tone at the top while defining and enforcing accountability and defines a continuous process and part of daily activities.

The risk IT framework is developed into a comprehensive process model that is depicted in Figure 1. The risk management process model consists

of three domains namely: RG, RE and RR. Each domain is divided to three processes and each process consists of several activities. The domains and their processes in risk IT framework are defined as:

- *RG*: The goal of RG is ensuring that IT risk management practices are embedded in the enterprise that enables it to secure optimal risk-adjusted return. RG domain has three main processes that are "establish and maintain a common risk view" RG1, "integrate with ERM" RG2 and "make risk-aware business decisions" RG3.
- *RE*: The aim of this domain is insuring that IT-related risks and opportunities are identified, analysed and presented in business terms. "Collect data" RE1, "analyse risk" RE2 and "maintain risk profile" RE3 are the main processes of this domain.
- *RR*: This domain ensures that IT-related risk issues, opportunities and events are addressed in a cost-effective manner and in line with business priorities. It is based on the following processes: "articulate risk" RR1, "manage risk" RR2 and "react to events" RR3.

Interested readers can be referred to [22] for more details about the domains, the processes and the activities introduced in risk IT framework.

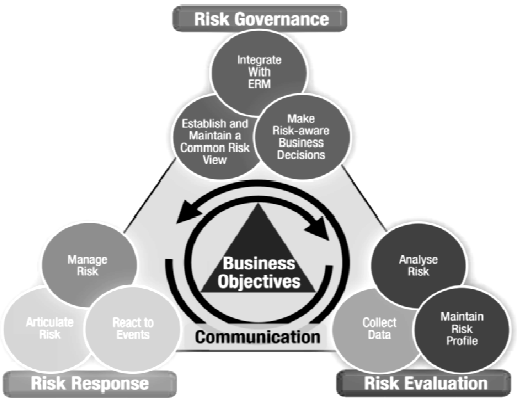

Figure 1. Risk IT framework [22].

4. The Proposed Methodology

4.1. Problem Definition

Most of the organizations try to determine their business policy and objectives regarding to the existing and potential risks. Risk management has a remarkable impact on strategic planning, decision making, avoiding adverse events and taking RR actions.

Iran Telecommunication Research Centre (ITRC) tends to improve the risk management processes for managing its IT projects. A process-oriented approach is adopted for managing risks in IT projects. The main processes of IT risk framework developed by ISACA [22], i.e., RG1, RG2, RG3, RE1, RE2, RE3, RR1, RR2 and RR3 are considered to develop the proposed methodology.

Several IT-related scenarios that can improve the maturity level of the risk management processes in IT projects are identified by the Chief Information Officer (CIO), the Chief Risk Officer (CRO) and the enterprise risk committee. The listed of these scenarios are presented in the first column of Table 1. Staff training scenario contains the design and implementing training, especially about IT-related risks and IT-related issues to improve staff knowledge. Renovation and upgrading equipment and technical infrastructure of IT are considered as equipment purchasing scenario. Changing central structure in ITRC is considered to define new and more applicable functions. A scenario is also defined to outsource ITRC projects to organizations that are empowered to certain issues related to the outsourced projects.

Table 1. Data for effectiveness of projects on risk processes (percent).

Scenarios	RG1	RG2	RG3	RE1	RE2	RE3	RR1	RR2	RR3
Staff Training	100	90	100	70	100	70	90	100	100
Purchase of Equipment	40	100	40	80	100	100	80	70	80
Changing Central Structure	70	80	80	90	40	60	80	70	70
Outsourcing ITRC Projects	20	30	10	20	10	20	20	80	90
Redesigning ITRC Processes	90	100	100	100	40	80	90	100	90
Implementation of New Office Automation Systems	50	100	30	40	60	80	60	50	60
Involving all Staff in all Phases of IT Project Management	70	90	90	50	60	50	60	60	100
Using the Outside Project Managers	10	20	30	10	50	20	40	60	30
Electronic Communication Between Contractors and ITRC	20	90	70	90	90	100	70	80	100

The key topics related to one of the scenarios are redesigning organization processes and the processes required to respond to stakeholder needs. Implementation of new office automation systems that have the ability to meet the needs of stakeholders is also considered as a scenario. One of the scenarios relies to change management that involves all related staff in implementing IT projects.

As a scenario, ITRC can be used the outside managers that are empowered to manage, conduct and implement IT projects. Finally, electronic communication among contractors, executors, advisors in ITRC may have a positive impact on risk management in IT projects. Therefore, it is also considered as scenario.

We conduct a series of meeting and interviews with ten experts who are familiar with enterprise risk management and IT risk management. Their opinions and judgments are obtained based on the amount of improvements in the maturity level of IT risk processes when implementing each scenario. The experts made the decisions based on their experiences on the similar works. Finally, the data are gathered and aggregated by some modifications. The final data which vary from zero to 100 percentages are reported in Table 1. The mentioned scenarios have a significant and positive impact on the maturity level of risk management processes. For example, implementing staff training scenario can increase the maturity level of RG2 process by 90 percent. Further, implementing this scenario may increase the maturity level of remaining risk IT processes, i.e., RG1, RG3, RE1, RE2, RE3, RR1, RR2, and RR3, by 100, 100, 70, 100, 70, 90, 100, and 100 percentages, respectively.

4.2. The Synthesis of DEA Concepts for Performance Evaluation and Improvement

The purpose of this paper is to select the best scenario (s) which improves the risk management processes in IT projects. To do so, DEA-based approach is adopted to measure the efficiency of scenarios. The proposed approach applies the DEA concepts to improve the maturity level of risk management processes in IT projects. Efficiency calculation using DEA models requires defining input and output variables and DMUs. Each scenario can be viewed as a DMU and each risk process can be considered as an output. Each scenario implementation can be increased the maturity level of risk processes; therefore, the risk processes can be viewed as output variables. Also, there are no explicit inputs in our problem. Therefore, one dummy input of 1 is considered for all the DMUs. Figure 2 indicates how our problem can be defined in DEA terms. According to Figure 2, DEA-WEI model and DEA-WEI model without explicit inputs are proposed for performance measurement and improvement purposes.

	Input 1	.....	**Input *m***	**Output 1**	.....	**Output *s***
DMU1	x_{11}	.....	x_{1m}	y_{11}	.....	y_{1s}
DMU2	x_{21}	.....	x_{2m}	y_{21}	.....	y_{2s}
⋮	⋮	.....	⋮	⋮	.....	⋮
DMU*n*	x_{n1}	.....	x_{nm}	y_{n1}	.....	y_{ns}

DMUs	**Dummy Input**	**Output 1(RG1)**	**Output 2(RG2)**	.....	**Output 9 (RR1)**
Scenario 1	1	y_{11}	y_{12}	.....	y_{1s}
Scenario 2	1	y_{21}	y_{22}	.....	y_{2s}
⋮	⋮	⋮	⋮	.....	⋮
Scenario *n*	1	y_{n1}	y_{n2}	.....	y_{ns}

Figure 2. Defining the problem in terms of DEA concepts.

5. Results

DEA-WEI Equation 3 is applied to the data presented in Table 1. Equation 3 should be solved for each scenario. For example, the following linear programming is solved for the first scenario with respect to Equation 3:

$$\begin{aligned}
&Max\ \theta_1 = 100u_1 + 90u_2 + 100u_3 + 70u_4 + 100u_5 + 70u_6 + 90u_7 + 100u_8 + 100u_9 \ s.t.\\
&100u_1 + 90u_2 + 100u_3 + 70u_4 + 100u_5 + 70u_6 + 90u_7 + 100u_8 + 100u_9 \le 1, 40u_1 + 100u_2\\
&+40u_3 + 80u_4 + 100u_5 + 100u_6 + 80u_7 + 70u_8 + 80u_9 \le 1, 10u_1 + 80u_2 + 80u_3 + 90u_4 + 40u_5\\
&+60u_6 + 80u_7 + 70u_8 + 70u_9 \le 1, 20u_1 + 30u_2 + 10u_3 + 20u_4 + 10u_5 + 20u_6 + 20u_7 + 80u_8 +\\
&90u_9 \le 1, 90u_1 + 100u_2 + 100u_3 + 100u_4 + 40u_5 + 80u_6 + 90u_7 + 100u_8 + 90u_9 \le 1, 50u_1 +\\
&100u_2 + 30u_3 + 40u_4 + 60u_5 + 80u_6 + 60u_7 + 50u_8 + 60u_9 \le 1, 70u_1 + 90u_2 + 90u_3 + 50u_4 +\\
&60u_5 + 50u_6 + 60u_7 + 60u_8 + 100u_9 \le 1, 10u_1 + 20u_2 + 30u_3 + 10u_4 + 50u_5 + 20u_6 + 40u_7 +\\
&60u_8 + 30u_9 \le 1, 20u_1 + 90u_2 + 70u_3 + 90u_4 + 90u_5 + 100u_6 + 70u_7 + 80u_8 + 100u_9 \le 1,\\
&u_1, u_2, ..., u_9 \ge \varepsilon > 0
\end{aligned} \tag{5}$$

To assess the efficiency of the second scenario, just the objective function of the above model revises and the constraints do not change. Therefore, the efficiency of the second scenario can assess by solving the following linear program:

$$\begin{aligned}
&Max\ \theta_2 = 140u_1 + 100u_2 + 40u_3 + 80u_4\\
&+100u_5 + 100u_6 + 80u_7 + 70u_8 + 80u_9\\
&s.t.\ \text{All constraints of model (5)}
\end{aligned} \tag{6}$$

Finally, the efficiency scores of all scenarios are obtained by solving nine linear programing models, i.e., one linear programing model for each scenario. The DEA-WEI results are reported in the second and third columns of Table 2. According to the results, 6 out of 9 scenarios (DMUs), i.e., staff training, purchase of equipment, redesigning ITRC processes, implementation of the new office automation system, involving all staff in all phases of IT project management and electronic communication between contractors and ITRC, receive the efficiency score of 1. Therefore, DEA-WEI Equation 3 cannot discriminate all efficient DMUs and provide full ranking vector of DMUs. To alleviate this problem, AP DEA-WEI Equation 4 is solved for each efficient scenario. As an example, we must eliminate the first constraint that bounds the efficiency score, namely constraint (5-2) in this case, to measure the AP efficiency score of the efficient scenario 1. It is performed by solving the following model.

Table 2. DEA results.

DMUs	**Results of Equation 3**		**Results of Equation 4**	
	Efficiency	**Rank**	**Efficiency**	**Rank**
Staff Training	1	1	1.4865	1
Purchase of Equipment	1	1	1.1029	4
Changing Central Structure	0.9074	7	0.9074	7
Outsourcing ITRC Projects	0.9	8	0.9	8
Redesigning ITRC Processes	1	1	1.2113	2
Implementation of New Office Automation Systems	1	1	1	5
Involving all Staff in all Phases of IT Project Management	1	1	1	5
Using the Outside Project Managers	0.6	9	0.6	9
Electronic Communication between Contractors and ITRC	1	1	1.1393	3

$$\begin{aligned}
&Max\ \theta_1 = 100u_1 + 90u_2 + 100u_3 + 70u_4\\
&+100u_5 + 70u_6 + 90u_7 + 100u_8 + 100u_9\\
&s.t.\ \text{All constraints of model (5)}
\end{aligned} \tag{7}$$

The related results of solving Equation 4 are presented in the fourth and fifth columns of Table 2. As it shows, the staff training scenario is achieved the maximum efficiency score that is 1.4865. Redesigning ITRC processes and electronic communication between contractors and ITRC are two next scenarios that receive the maximum efficiency scores among scenarios. Their efficiency scores are 1.2113 and 1.1393, respectively. The last column presents the ranking vector of DMUs.

Since, the resources are limited in Information and Communication Technology (ICT) sectors, selecting and implementing appropriate scenarios are very important in strategic environment [11]. Therefore, ITRC selects one or some of the best scenarios considering the IT budget limitations. For example, when the staff training scenario is accepted for implementation, ITRC should be trained its staff regarding RG, risk analysis and RR practices.

With respect to RG domain, all staff in risk management positions should be trained in critical risk

management techniques (e.g., standard risk analysis techniques, crisis management, project management, skills of people [audit, etc.,] to detect when something IT-related is amiss). Risk awareness training should be included situations and scenarios beyond specific policy and structures and promoted a common language for communicating risk. All staff in risk management positions should be trained in IT risk assessment, IT risk tolerance thresholds, IT risk aware culture, effective communication of IT risk, and enterprise risk practices.

With respect to RE domain, RE training should be performed based on an agreed upon plan and informal training on the job occurs. RE training includes techniques beyond minimum policy and common tools to determine the business relevance of risk factors. Enterprise risk managers and business processes owners receive targeted IT risk analysis training and the training on how to collect data on the operating environment and risk events, maintain and support risk profile, estimate IT risk, identify RR options and develop IT risk indicators.

With respect to RR domain, employees should be periodically trained in IT-related threats, risk scenarios and controls relevant to their roles and responsibilities. RR training should be provided on the basis of an agreed-upon plan, and informal training occurs on the job. Enterprise risk managers and business process owners and related staff in risk management positions should be trained on how to communicate IT risk analysis results, report IT risk management activities and state of compliance, interpret independent IT assessment findings, identify IT-related opportunities, monitor operational alignment with risk tolerance thresholds, respond to discovered risk exposure and opportunity, implement controls, report IT risk action plan progress, react to events, maintain incident response plans, monitor IT risk, initiate an incident response, communicate lessons learned from risk events.

6. Concluding Remarks

Managing IT projects require more complex practices than those of traditional projects, since the traditional projects produce physical and tangible outputs while the outputs of IT projects are qualitative and intangible. Moreover, structured and organized ways exist to manage traditional projects while these ways may not be applicable to all aspects of IT projects. Therefore, the need for risk management is widely recognized in IT projects and performing risk management plays an important role in fulfilment of IT projects. In this paper, the most recent risk IT framework introduced by ISACA [22] is adopted to develop our proposed approach. Several scenarios are designed to improve the maturity level of the existing risk IT processes in the ITRC organization. Moreover, two DEA models are modified in the context of our problem and then applied to evaluate the designed scenarios in the ITRC organization.

Acknowledgements

The authors gratefully acknowledge the financial support of the Cyber Space Research Institute (CSRI), Iran, under project number 9232433 in 2012. We are also grateful to the anonymous reviewers for their valuable comments and constructive criticism.

References

[1] Alhawari S., Karadsheh L., Nehari Talet A., and Mansour E., "Knowledge-Based Risk Management Framework for Information Technology project," *the International Journal of Information Management*, vol. 32, no. 1, pp. 50-65, 2012.

[2] Andersen P. and Petersen C., "A Procedure for Ranking Efficient Units in Data Envelopment Analysis," *Management Science*, vol. 39, no. 10, pp. 1261-1264, 1993.

[3] Baccarini D., Salm G., and Love D., "Management of Risks in Information Technology Projects," *Industrial Management and Data Systems*, vol. 104, no. 4, pp. 286-295, 2004.

[4] Bandyopadhyay K., Mykytyn P., and Mykytyn K., "A Framework for Integrated Risk Management iin Information Technology," *Management Decision*, vol. 37, no. 5, pp. 437-444, 1999.

[5] Benaroch M., Lichtenstein Y., and Robinson K., "Real Options in Information Technology Risk Management: An Imprical Validation of Risk-Option Relationships," *MIS Quarterly*, vol. 30, no. 4, pp. 827-864, 2006.

[6] Chapman B. and Ward C., *Project Risk Management*, *Processes*, *Techniques and Insights*, John Wiley, 2003.

[7] Charnes A., Cooper W., and Rhodes E., "Measuring the Efficiency of Decision Making Units," *the European Journal of Operational Research*, vol. 2, no. 6, pp. 429-444, 1978.

[8] Cooper W., Seiford M., and Tone K., *Data Envelopment Analysis: A Comprehensive Text with Models, Applications, References and DEA-Solver Software*, Kluwer Academic Publishers: Boston, 2000.

[9] Dey K. and Kinch J., "Risk Management in Information Technology Projects," *the International Journal of Risk Assessment and Management*, vol. 9, no. 3, pp. 311-329, 2008.

[10] Dey K., Tabucanon T., and Ogunlana O., "Planning for Project Control Through Risk Analysis; A Case of Petroleum Pipeline Laying

Project," *the International Journal of Project Management*, vol. 14, no. 4, pp. 231-240, 1996.

[11] Fasanghari M., Amalnick S., Chaharsooghi K., and Ko S., "The Fuzzy Evaluation of the Ict Projects in Strategic Environment (Case Study: Iran Telecommunication Research Center)," *the International Journal of Information Technology and Decision Making*, vol. 10, no. 5, pp. 873-890, 2011.

[12] Guiling L. and Xiaojuan Z., "Research on the Risk Management of IT Project," *in Proceedings of International Conference on E-Business and E-Government (ICEE)*, pp. 2542-2545, 2011.

[13] Hatefi M. and Jolai F., "A New Model for Classifying Inputs and Outputs and Evaluating The Performance of Dmus based on Translog Output Distance Function," *Applied Mathematical Modelling*, vol. 34, no. 6, pp. 1439-1449, 2010.

[14] Hatefi M. and Torabi A., "A Common Weight MCDA-DEA Approach to Construct Composite Indicators," *Ecological Economics*, vol. 70, no. 1, pp. 114-120, 2010.

[15] Hedelin L. and Allwood M., "IT and Strategic Decision-Making," *Industrial Management and Data System*, vol. 102, no. 3, pp. 125-135, 2002.

[16] Hongxia W. and Baihua T., "IT Project Risk Assessment Model Based on Fuzzy-AHP, " *in Proceedings of the 2nd International Conference on Information Engineering and Computer Science*, Wuhan, pp. 1-4, 2010.

[17] Hope C., Parker J., and Peake S., "A Pilot Environmental Index for the UK in the 1980s," *Energy Policy*, vol. 20, no. 4, pp. 335-343, 1992.

[18] Huang M., Lu Q., Ching K., and Siu K., "A Distributed Decision Making Model For Risk Management of Virtual Enterprise," *Expert Systems with Applications*, vol. 38, no. 10, pp. 13208-13215, 2011.

[19] Huang S., Chang C., Shing-Han H., and Lin T., "Assessing Risk in ERP Projects: Identify and Prioritise the Factors," *Industrial Management and Data Systems*, vol. 104, no. 8, pp. 681-688, 2004.

[20] ISACA Committee, CobiT 4.1., IT Governance Institute, available at: http://www.isaca.org.ua/index.php/homepage/download/category/2-standards?download=6:cobit-4-1-eng, last visited 2007.

[21] ISACA Committee, Enterprise Value: Governance of IT Investments, The Val IT Framework 2.0., IT Governance Institute, available at: https://www.isaca.org/Knowledge-Center/Val-IT-IT-Value-Delivery-/Documents/Val-IT-Getting-Started-Jul-2008.pdf, last visited 2008.

[22] ISACA Committee, The Risk IT Framework., IT Governance Institute, USA, 2009.

[23] Johnson J., "Chaos: The Dollar Drain of it Project Failures," *Application Development Trends*, vol. 2, no. 1, pp. 41-47, 1995.

[24] KarimiAzari R., Mousavi N., and Mousavi F., and Hosseini B., "Risk Assessment Model Selection in Construction Industry," *Expert Systems with Applications*, vol. 38, no. 8, pp. 9105-9111, 2011.

[25] Li J., Li M., Wu D., and Song H., "An Integrated Risk Measurement and Optimization Model for Trustworthy Software Process Management," available at: http://www.sciencedirect.com/science/article/pii/S0020025511005354, last visited 2012.

[26] Liu P., Zhang X., and Liu W., "A Risk Evaluation Method for the High-Tech Project Investment based on Uncertain Linguistic Variables," *Technological Forecasting and Social Change*, vol. 78, no. 1, pp. 40-50, 2011.

[27] Liu B., Zhang Q., Meng W., and Xu F., "A Study of DEA Models without Explicit Inputs," *Omega*, vol. 39, no. 5, pp. 472-480, 2011.

[28] Lo C. and Chen J., "A Hybrid Information Security Risk Assessment Procedure Considering Interdependences Between Controls," *Expert Systems with Applications*, vol. 39, no. 1, pp. 247-257, 2012.

[29] Mathrani S. and Mathrani A., "Utilizing Enterprise Systems for Managing Enterprise Risks," *Computers in Industry*, vol. 64, no. 4, pp. 476-483, 2013.

[30] Michalk W. and Blau B., "Risk in Agreement Networks," *Information Systems and e-Business Management*, vol. 9, no. 2, pp. 247-266, 2011.

[31] Mustafa A. and Al-Bahar F., "Project Risk Assessment using the Analytic Hierarchy Process," *IEEE Transaction on Engineering and Managment*, vol. 38, no. 1, pp. 46-52, 1991.

[32] Othman M., "Fuzzy Comprehensive Evaluation for IT Project Risk Management," available at: http://www.scientific.net/AMM.229-231.2753, last visited 2012.

[33] Rainer K., Snyder A., and Carr H., "Risk Analysis for Information Technology," *the Journal of Management Information Systems*, vol. 8, no. 1, pp. 129-147, 1991.

[34] Rotaru K., Wilkin C., Churilov L., Neiger D., and Ceglowski A., "Formalizing Process-Based Risk with Value-Focused Process Engineering," *Information Systems and e-Business Management*, vol. 9, no. 4, pp. 447-474, 2011.

[35] Ruch M. and Sackmann S., "Integrating Management of Customer Value and Risk in E-Commerce," *Information Systems and e-Business Management*, vol. 10, no. 1, pp. 101-116, 2010.

[36] Schmidt R., Lyytinen K., Keil M., and Cule P., "Identifying Software Project Risks: An international Delphi study," *the Journal of*

Management Information Systems, vol. 17, no. 4, pp. 5-36, 2001.

[37] Seyedhoseini M. and Hatefi A., "Two-Pillar Risk Management (TPRM): A Generic Project Risk Management Process," *Scientia Iranica*, *Transaction E*: *Industrial Engineering*, vol. 16, no. 2, pp. 138-148, 2009.

[38] Seyedhoseini M., Noori S., and Hatefi A., "An Integrated Methodology for Assessment and Selection of the Project Risk Response Actions," *Risk Analysis*, vol. 29, no. 5, pp. 752-763, 2009.

[39] Stoneburner G., Goguen A., and Feringa A., "Risk Management Guide for Information Technology Systems," *Technical Report*, NIST Special Publication, 2002.

[40] Tummala V., Rao M., and Leung H., "Applying a Risk Management Process (RMP) to Manage Cost Risk for an EHV Transmission Line Projects," *International Journal of Project Management*, vol. 17, no. 4, pp. 223-235, 1999.

[41] Vitale R., "The Growing Risks of Information System Success," *MIS Quarterly*, vol. 10, no. 4, pp. 327-334, 1986.

[42] Wang S., "Designing Information Systems for E-Commerce," *Industrial Management and Data Systems*, vol. 101, no. 6, pp. 304-315, 2001.

[43] Wet D. and Visser K., "An Evaluation of Software Project Risk Management in South Africa," *South African Journal of Industrial Engineering*, vol. 24, no. 1, pp. 14-28, 2013.

[44] Williams M., "A Classified Bibliography of Recent Research Relating to Project Risk Management," *European Journal of Operational Research*, vol. 85, no. 1, pp. 18-38, 1995.

[45] Yang H., "Software Quality Management and ISO 9000 Implementation," *Industrial Management and Data Systems*, vol. 101, no. 7, pp. 329-338, 2001.

[46] Yucel B., Cebi S., Hoege B., and Ozok F., "A Fuzzy Risk Assessment Model for Hospital Information System Implementation," *Expert Systems with Applications*, vol. 39, no. 1, pp. 1211-1218, 2011.

[47] Zhang K., Guan J., "Distinguishing Attack on Common Scrambling Algorithm," *the International Arab Journal of Information Technology*, vol. 12, no. 4, pp. 410-414, 2015.

Morteza Hatefi received his BSc degree in statistics in 2005 and his MSc and PhD degrees in industrial engineering from University of Tehran in 2009 and 2013, respectively. His current research interests include: Supply chain network design, logistics planning, multi-criteria decision making, data envelopment analysis, information technology, risk management, uncertain programming and operations research applications. He has published several papers in the aforementioned areas.

Mehdi Fasanghari received his BSc degree in industrial engineering in 2004 and his MSc degree in information technology engineering in 2006, Iran. Currently, he is a PhD student in industrial engineering department, University of Tehran, Iran. His current research interests are IT Governance, E-government promotion, enterprise architecture, interoperability, soft computing, intelligent decision support systems and advanced multi-criteria decision analysis. He has published more than 50 conference and 20 journal papers in this regard and he is the editor of international journals and IEEE conferences. He has been involved in many scientific and managerial positions such as deputy head of IT Research Faculty at Cyber Space Research Institute these years.