ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

A RISK MITIGATION DECISION FRAMEWORK FOR INFORMATION TECHNOLOGY ORGANIZATIONS

NORAINI CHE PA, BOKOLO ANTHONY JNR., YUSMADI YAH JUSOH, ROZI NOR HAIZAN NOR, TEH NORANIS MOHD ARIS
Faculty of Computer Science and Information Technology, University Putra Malaysia, 43400 UPM, Serdang, Selangor, Malaysia.
E-mail: norainip@upm.edu.my, result4real@yahoo.com, yusmadi@upm.edu.my, rozi@upm.edu.my,
E-mail: nuranis@upm.edu.my

ABSTRACT

Information technology (IT) organizations are faced with various risks such as strategic, operational and technical risks. These risks should be identified, measured and mitigated. Risk mitigation gives an opportunity to IT practitioners and management to compute risks and develop suitable strategies to treat the risk. Risk mitigation in organizations provides a disciplinary environment for decision making to measure and treat potential risk continuously. Existing model and frameworks provides inadequate support to practitioners in making risk decision pertaining risk mitigation. This is due to the fact that existing models or frameworks lacks the capabilities to support practitioners. In order to address this challenge, this research identifies the processes and components of risk mitigation in organization's and proposes a framework of risk decision for mitigating both technical and operational risk using software agents and knowledge mapping as techniques. Qualitative research was adopted using interview to collect data. A pilot study was carried out to validate the instrument. The case study was later carried out to verify the risk mitigation process and components. Lastly the framework was evaluated using iterative triangulation.

Keywords: *Risk Decision, Risk Mitigation, Software Agent, Knowledge Mapping, Iterative Triangulation*

1. INTRODUCTION

In information technology (IT) organizations, risk management is defines, measures, and controls uncertain events for reducing many losses as possible, and to optimize IT infrastructure. Thus, IT practitioners must learn to treat the possible undesirable effects of risk against the possible advantages of its related opportunity [1]. Risk management involves approaches to uncover potential risks, to predict losses, and to take proper action to prevent and control risk [2]. Risk mitigation is defined as the process of identifying risk and selects suitable solutions to reduce risk according to the objectives of the practitioners (experts, IT managers, staffs, decision makers) [3]. Risk mitigation includes monitoring, tracking and evaluating risk process effectiveness throughout the utilization of IT infrastructures. With effective mitigation of risk, the return of IT project can be optimized to prolong business strategies and goal [4].

The mitigation includes the stepwise execution of the risk method that provides a mechanism for practitioners to handle risk effectively [3]. Risk mitigation can be said to be an important process to assist practitioners attaining the changes of business, future investment and information system [5]. Risk mitigation is also a sequence of phase's aims at identifying, addressing, and reducing risk before turn into either threat or effective IT operation in organizations [6].

Decision making is an important task for any organizations for assuring they can be sustained and survived in the long term. Therefore each organization must be capable of making good decisions. Poor decision making by IT practitioners in risk mitigation is due to practitioners' unwillingness to rely on others for making decisions, not taking ownership of decisions, conflicting priorities and unstable staff availability of decision [7]. Decision making in risk mitigation involves for recognizing, generating alternative solutions, choosing among alternatives, and implementing the chosen alternative of risks [8]. In risk mitigation, decision making is important to align the organization policy and procedure structure. In addition, it is reliant on the quality of decisions that informs its operation. If decisions are right, it translates to positive organizational outcomes, but if wrong decisions are made it may ruin the organization. A suitable decision making process can support organizations for increasing the effectiveness, incorporating understanding, communication and effective management [9]. Risk mitigation aids IT managers to know the mutual relationships among the enablers of risks mitigation and provides a suitable metric to quantify these risks [3]. The purpose of this paper is to present a framework proposed for risk decision mitigation in IT organizations to assist IT practitioners in making decision and mitigating risk.

The structures of the paper are as follows: Section 1 is the introduction to this research. Section 2 presents the related works to this research topic which is the risk mitigation. Section 3 is about the methodology applied to conduct this research. Next, section 4 presents the formulation of the proposed framework and section 5 provides the results of the data collection and analysis. Finally, section 6 is the discussion and conclusion.

2. RESEARCH BACKGROUND

This section briefly explores the research problem, the importance of risk decisions, related works and lastly an overview of knowledge mapping and multi software agents.

The main problem emerging in the field of risk mitigation in IT organization is mainly due to existing approaches not being able to provide adequate support to practitioners in mitigating risk. The secondary study from the literature revealed that increasing complexity of IT processes and the continuous growth of risk in IT organization shows that critical decisions on mitigating operational and technical risk in IT infrastructures must be made as early as possible, once the risk is identified [10][11]. Mitigating technical and operational risks is a limitation and the main obstacle to secure a successful IT project implementation. The identified problem of mitigating risk in IT organization includes lack of risk decision in risk mitigation and inadequate support and lack of capabilities to support practitioners.

Decisions are performed to mitigating risk in IT organizations. Practitioners make decisions to solve operational and technical risk. However, existing approaches can't provide assistance for practitioners to make risk decisions on treating identified risk [12]. Therefore, risk mitigation is not properly carried out, since the risk decisions are basically ignored by practitioners. Currently, mitigating risk in IT organizations is failed due to inadequate support from the lessons learnt; best practices and expertise to mitigate risk [13][10]. Risk mitigation practitioners can derive benefits through the sharing and reuse of historical data, extracted from past projects which are lacking in existing risk mitigation approaches [14]. Furthermore, existing approaches are lacking capabilities to support practitioners in mitigating the risk and reuse the knowledge to identify and mitigate the risks [15].

Information has become an essential resource for decision making process in order to emphasize organizational abilities to manage opportunities and risks [16]. A decision is the act of reaching a conclusion or making up one's mind [17]. Strategic decisions affect key factors which control the success of an organization's strategy. In contrast with tactical decisions, that affects the day-to-day execution of steps required to attain these goals.

The effectiveness of IT organizations is dependent on the quality of decisions. The right decisions are translated in positive organizational outcomes, but poor decisions resulting from insufficient or inaccurate information, such organization could be ruined. Therefore, the risk decision is a major determining factor of mitigating risk in IT organization. Decision making has become an essential resource for managing organizations [16] and the defined risk decision process prevents to cause IT projects to overdue schedule, over budget and poor quality [9]. A good decision helps staffs, group or organization to become more effective and the opposite is its reverse. Every organization grows as a result of decisions made by its members. Decision making involved four phases: intelligence, design, choice and implementation [18]. Effective decision making is the most important and challenging task of a senior IT managerial responsibilities.

Risk decision aids practitioners for estimating the impacts of risks and subsequently develops suitable strategies to them. Besides that, risks mitigation helps IT managers and practitioners to have a robust comprehensive risks mitigation policy. Also, risks mitigation involves making the decision on how to treat the risk. Since IT organization is faced with risks such as operational, technical and strategic risk. These risks should be mitigated. However, risk mitigation is complicated, particularly in IT projects, leading to difficulty in choosing and executing mitigation actions. An effective risk mitigation plan can identify risks, thus providing useful decision support for IT managers [19]. Five activities involve in risk mitigation such as risk identification, assessing risk, plan and implementing solutions, conducting failure mode and effect analysis and lastly continuous improvement [20].

A qualitative method-based risk mitigation method was proposed using suitable safeguards such as prevention, reduction, monitor, detection, or correction and recovery to mitigate risk with risk analysis results. The model comprises of the result of the analysis, the safeguard methods, safeguard techniques, safeguard decision and safeguard implementation [21]. A model to evaluate and mitigate information systems (IS) development risk using balance score card was developed [22]. The model mitigate IS risks based on risk mitigation strategies put forward to transform the risk into strategic execution. The researchers claim the model has the advantage of integrating strategy and mitigating risk effectively using a balanced score card (BSC) as to reduce IS development risks and improving development performance while guaranteeing the realization of the target.

A model for IT and software risk mitigation plan to reduce the risks consequences and their occurrence probabilities was proposed by [23]. The model determines the mutual impacts of the risk mitigation activities and implements a risk mitigation plan. The researcher used case study to verify the performance of the model. The model is based on the verified and extracted data from information systems. This model process involves creating risk mitigation plan according to obtained information from the previous project and historical data, a mitigation plan should is designed. [24] designed a risk mitigation model in the small and medium enterprise (SME). The model purpose is to define a comprehensive structure of internal and external risks that exist in open innovation. The model competent to prevent the proper functioning of SMEs, and provide results on the factors that help mitigate the risks that occur in SMEs by using external knowledge to accelerate organizational and technological learning of a firm.

A model for risk mitigation in software management using the stepwise execution methodology which is consisted of an easy flowchart to express the working of each mitigation strategy against any risk is introduced. Then, the researchers proposed to index the risk factors by calculating the impact and likelihood of each risk factor [25]. Mitigation of software risk management process model and risk mitigation decision proposed to create new opportunities in taking consideration on the impacts of such hidden risks. The model uses a synthesized approach which identifies risks and opportunities together with the risk reduction activities in improving the risk mitigation decisions [12].

Knowledge Mapping and Multi-Software Agents

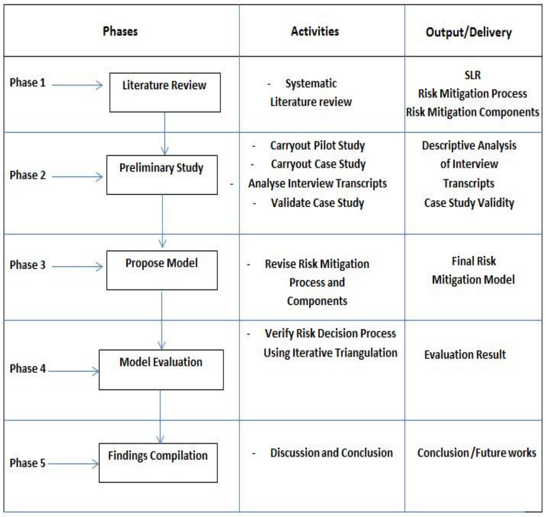
Knowledge is information in which data are extracted and stored them into databases so that it becomes suitable for input to a knowledge processor of some kind. Knowledge mapping in risk mitigation context is in its beginning and has the potential to address both functional and technical risks faced in IT projects that aims to improve the efficiency and effectiveness utilization of the organization's knowledge. Knowledge map is a picture of what exists in an organization or a network, and then providing some sort of list or picture that shows where to find it [26]. Therefore, it can be used as a technique to mitigate risk in IT organizations.

An agent is a soft-ware that acts or brings about a certain result; it is one who is empowered to act for another [13]. The agent is known as a software entity, which is autonomous to achieve its design objectives, considered as a part of an overall objective, through the axiom of communication and coordination with other agents [27]. The software system is a component that can interact autonomously as a substitute for its user with its environment and other agents to achieve the predefined goal [28].

There are some routines in software agents such as create, organize, store and use tacit knowledge embedded in individuals and practices. Software agents create and store explicit knowledge as declarative memory through mapping a process by which explicit knowledge is created from information and stored in repositories for repetitive and routine querying [29]. These agents capture tacit knowledge and convert it into explicit knowledge stored as best practices. Organizations need to allocate and rely on software agents (e.g., embedded algorithms that perform autonomous functions on behalf of the user) that perform core knowledge mapping activities. In knowledge mapping software agents increase process transparency by facilitating knowledge sharing and transfers, relieving the user of understanding inherent translation and conversion complexities.

3. RESEARCH METHODOLGY

This section discusses the methodology that has been considered in this research in sequence to address the research problem. The section describes the 5 phases which cover the research phase, activities and outputs. The research phases are~~:~~ literature review, preliminary study, model development, model evaluation, and findings and compilation.



Phases		Activities	Output/Delivery
Phase 1 →	Literature Review	- Systematic Literature review	SLR Risk Mitigation Process Risk Mitigation Components
Phase 2 →	Preliminary Study	- Carryout Pilot Study - Carryout Case Study - Analyse Interview Transcripts - Validate Case Study	Descriptive Analysis of Interview Transcripts Case Study Validity
Phase 3 →	Propose Model	- Revise Risk Mitigation Process and Components	Final Risk Mitigation Model
Phase 4 →	Model Evaluation	- Verify Risk Decision Process Using Iterative Triangulation	Evaluation Result
Phase 5 →	Findings Compilation	- Discussion and Conclusion	Conclusion/Future works

Fig. 1 Research Methodology

Figure 1 shows the research methodology. The explanation of this figure covers various activities, objectives, methods and outputs for each research phase in this paper. The phases, activities and output carried out in this paper are explained below.

a. Phase 1: Literature Review

Phase 1 encompasses the reviewing of journals, conference proceeding, books literatures on risk mitigation practices and process. This phase is important since it lays the foundation for the research background and framework development.

b. Phase 2: The Preliminary Study

This phase comprises data collection, case study selection, sampling method, pilot study, the case study by interview and data analysis using Nvivo. This phase is carried out to confirm the risk mitigation components and process derived from the literature. A pilot study is conducted to check if the informants understand the questions in the instrument. It allows the researcher to determine the adequacy of instructions to the informants.

c. Phase 3: Proposed Framework

This phase includes the development of the risk decision mitigation framework. The framework will assist in risk decision in mitigating operational and technical risk in IT organizations using multi-software agents and knowledge mapping as techniques.

d. Phase 4: Model Evaluation

Phase 4 involves the evaluation of the developed framework using the Iterative triangulation method. In this phase, the data from the case studies were compared and triangulated to the findings from the literature. Also, a risk mitigation document from one of the organizations used for the case study was analyzed and related to the risk decision process in the proposed framework.

e. Phase 5: Findings Compilation

Phase 5 involves the conclusion of this research paper by highlighting the contributions of the paper and stating future works.

4. PROPOSED FRAMEWORK

Based on the finding from the literature and the confirmation of these findings via the case studies, the risk mitigation framework comprises risk identification, risk decision, risk treatment, risk monitoring and risk report. The risk mitigation report is a new process added based on the suggestions of the informants from the case studies. The process involves converting the data from the knowledge base and generates the risk mitigation report to PDF file format for the practitioners and decision makers. The risk generated report retrieved operational and technical risk data from the knowledge base for the practitioners to analyze. It comprises user manual, risk magnitude estimation and risk advice/documentation on risk mitigation.

The framework for risk decision for mitigating risk in IT organizations is shown in Figure 2. The framework comprises the risk mitigation process, risk mitigation components, software agents and knowledge mapping.

The risk mitigation decision framework is proposed to:

a. Assists in decision making relating to risk mitigation in IT organization. The framework will treat and monitor risk in IT organizations. Result from this research is a novel process for identifying, treating and monitoring operational and technical risk in IT organization through which information is retrieved and passed via knowledgebase in order to assist in decision making process for mitigation risk in IT process.

b. Supports risk mitigation by measuring the probability of risky events and the losses. Also, the framework assists in computing the risks so that the practitioners can understand the contribution of risks.

c. Supports for monitoring and communicating of risk among practitioners to verify whether their efforts to mitigate these risks are yielding the desired results or not. This would help the decision makers and practitioners to estimate the impacts of various risks a consequently choose solutions to treat the risk.

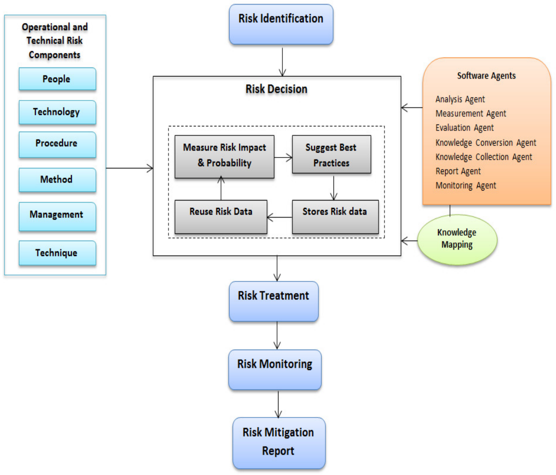


Fig 2. A Risk Mitigation Decision Framework for an IT Organization

The framework is mainly based on the risk decision which includes risk impact and probability measurement, best practice suggestion, risk data storage and reusing of risk data. The risk decision is the area of concentration in this research based on the research problem mentioned in section 2. The risk decisions will assist in answering the research problems in this research. The framework provides support for practitioners through the risk mitigation report. Using the components, software agents and knowledge mapping, decision making can be carried out by practitioners' in mitigating risk in IT organization. The framework supports risk decision and aids knowledge retrieving, storing, sharing and updating process of risk mitigation. The framework has the capabilities to support practitioners in mitigating risks in IT organization by capturing and reusing the lessons learnt from previous risk mitigation, case studies and best practices, to utilize and share the previous as well as existing knowledge and experience within practitioners.

The components are the same as the operational and technical risk; they combine with the software agents and knowledge mapping for carrying out risk decisions for mitigating risk in IT organization. The components people, techniques, methods, management, technology and procedure are used for the risk decision in mitigating risk using the mapping of knowledge and multi-software agents which are the analysis agents, risk measurement agent, evaluation agent, knowledge collection agent, knowledge conversion agents, monitoring agent and report agent. Thus, risk decision is the main process in the risk mitigation model where the decision is carried out based on various alternatives or solutions on how to treat the risk. The risk mitigation component people, technology, technique, management, procedure and methods influences risk decision, thus risk decision relies on the other components. Where a risk decision is the existing approach used in IT organization for making the decision for mitigating the risk [30].

A. Risk Decision

The risk decisions are the main problems in mitigating risk based on the research problem stated in this paper, thus the risk decision sub-processes are discussed below.

i. Risk Impact and Probability Measurement

Risk impact and probability measurement are the systematic process to understand the nature of the risk/risks (by finding, recognizing and describing risks) and to deduce the level of risk (by assigning values to impact and their probability). Risk impact and probability measurement provide the basis for risk decisions about risk treatment. During the risk decision phase, practitioners have to consider each identified risk and make a judgment about the probability and impact of that risk. Normally, practitioners depend on their judgment and experience of past projects and their problems. Once the risks have been measured and ranked, practitioners can make decisions on which of these risks are most significant. Risk decisions depend on a combination of the probability of the risk arising and the impact of that risk. In general, the most serious risks should always be considered, as should all serious risks that have more than a moderate probability of occurrence.

ii. Best Practice Suggestion

Best practices are based on past risk mitigation cases gotten by capturing information and identifying critical success and failure factors in risk decisions. A knowledgebase of risk operational and technical risk identified was populated with a summary of both internally and externally used case studies. A description of the risks comprising risk event drivers, mitigation strategies implemented, risk impact and probability constitute the database of case studies. Therefore, practitioners will be able to locate past risk mitigation activities via a collaborative environment or a risk mitigation system.

iii. Risk Data Storage

The knowledge base is information captured from practitioners' know-how, lessons learnt, case studies, best practices and risk mitigation standards. The knowledge is capable of facilitating the use of past successes and failures, captured to mitigate risks in IT governance. The knowledge stored the lessons learnt of case-based studies on experiences. The risk decision can be enhanced through considering successes and failures of previously finished risk mitigation. Indeed, a success factor can be resulting from historical lessons learnt; otherwise previous mistakes can be repeated leading to failures. Moreover, the lessons learnt also help identify the location of critical risk items which are identified based on success factors from lessons learnt.

iv. Reusing of risk data

The reuse of risk data provides a possibility for transferring excellence from several sources into the risk mitigation process. It also assists to populate the database with respect to identification of operational and technical risk and mitigation strategies. Additionally, data can be reused from different aspects of IT governance depending on the specific role in the team, background, experience and personality. Reusing of risk data is designed to generate lessons learnt and build onto the knowledge on completion of each risk decision.

The risk decision process in Section 5.1 above assists to address and solve the research problem in this paper.

B. Multi-Agents for Risk Decision Mitigation

The risk decision mitigation framework has been developed using software agents and knowledge mapping as seen in Figure 4. Seven software agents are incorporated to assist in risk decisions in mitigating operational and technical risk in IT organization. These agents will be used to develop the risk mitigation system (RMS) tool. Table 4 briefly describes the roles of the multi-software agents in the developed framework;

C. Knowledge Mapping for Risk Decision Mitigation

Mapping process involves storing data into the knowledge base and for its database maintenance. Knowledge Mapping is used in this process to store risk mitigation strategies in knowledge base. It may update existing knowledge which is outdated and not in use and also can remove the knowledge that is determined by experts. The use of knowledge map, agents can retrieve relevant knowledge for decision makers more effectively, because the knowledge map shows the relationship between knowledge and their usage. A knowledge map provides indexes the real knowledge that illustrations where to find resources and knowledge [31]. Knowledge map transforms tacit knowledge into explicit knowledge that can be displayed in texts, categories, and graphics. The knowledge mapping is applied the mind mapping to build a knowledge map that can be easily understood by staff and management in the organizations.

5. FRAMEWORK EVALUATION

The evaluation of the framework involves verifying the risk decision process using iterative triangulation, by verifying the risk decision process based on a set of questions. This phase also involves using the risk mitigation document in Appendix from the first organization in the case studies.

Overview of Iterative Triangulation

The risk decision process was verified using the Iterative Triangulation method. The risk decision process in the risk mitigation model comprises of four processes, namely; measure risk impact & probability, suggest best practices, stores risk data and reuse risk data. The verification indicates that the risk decision process is able to solve the research problems, which is to address the lack of risk decision in risk mitigation and to provide adequate support to practitioners in mitigating risk in IT organization. Thus, in order to solve the research problem, a framework of risk mitigation is proposed which assist practitioners in risk decisions and provides support in mitigating risk in IT organization, there is need to provide answers to two questions:

- What is the right qualitative acceptance level to describe these processes?
- Based on the qualitative acceptance level, can a formula be proposed to indicate the level of risk decision in mitigating risk in IT organization?

The solution to the problem can be found by using a method based on Iterative Triangulation Method [32] [33]. This method employs systematic iteration between literature review, case studies and intuition in order to develop a new theory or technique. This method involves four phases as described below in Figure 3 which are: groundwork (review literature in order to select cases), induction (analyze cases in order to shape conjectures), iteration (refine theory) and conclude (evaluate theory and suggest future research direction).

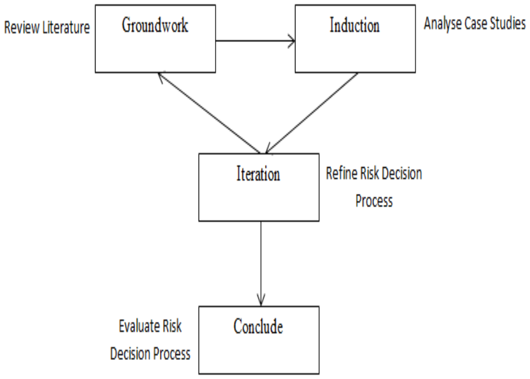


Fig 3. Iterative Triangulation Method

Phase 1- Groundwork

Groundwork phase involves the review literature in order to select the case study. This phase is carried out where the existing literature of risk mitigation was reviewed in details to identify the current process of risk decision in mitigating risk in IT Governance.

Phase 2 – Induction

Next, the induction phase conducted to analyze cases in order to shape conjectures. This phase involves selecting the case study, analysis of the case study and shapes conjure. In order to identify the risk decision process, the same organization was used by carrying out a follow-up interview to compare findings from both case studies, where this study involves 2 different organizations that practice risk mitigation in their projects, with a total of 7 informants. The first 4 informants are from case study 1, where the informants are currently the Head of Division Planning and Governance, ICT Security Officer, Head of Policy and Governance and Head of Project in Data Centre in the organization as stated in Section 4.2. The remaining 3 informants are from case study 2 where they are currently the Head of ICT Services and Governance in the institution, Head of ICT Development and ICT Director of the organization.

The case study was analyzed in order to verify the risk decision process. Below are the findings from case study 1 and case study 2, the findings below validates the risk decision process in the risk mitigation model. The data from the follow up interview from the 7 informants from the 2 case studies is stated below. It can be seen that the findings is aligned with the risk decision process which includes; measures risk impact and probability, suggest best practices, stores risk data and reuse risk data. Thus, it can be seen that the data from the 2 case studies are triangulated since both findings are similar as shown below;

Findings from Case Study 1

Below are the findings from case study 1 is based on the risk decision process;

a. Measures Risk Impact and Probability

Presently the organization has a ISMS, that is also used by the committee to classify the risk based on high, medium and low as stated above. The organization mitigates risk by evaluating the risk based on risk rating (high, medium and low) using MyRAM application, the informants also mentioned that the decision is based on the evaluation of the risk (high, medium or low), after which the decision makers propose the risk mitigation control based on the identified risk impact. They proceed to calculate the risk, then they analyze the risk control and presents the report from MyRAM application, which is later presented to the management.

b. Suggest Best Practices

The decision making uses historical information to show the past and predict the future.

c. Stores Risk Data

Thus the organization only prints the risk documents and stores the risk assessment and mitigation report as hard copy.

d. Reuse Risk Data

The risk assessment team uses knowledge source, documents in hard copy format but not software, since all the past risk assessment and mitigation are stored in a file cabinet in the organization.

Findings from Case Study 2

Below are the findings from case study 2 based on the risk decision process;

a. Measures Risk Impact and Probability

However, the organization don't use any risk formulated to calculate and mitigate the risk, the committee key in the risk manually and calculates the risk manually, thus the informant agrees that an advance system will help to calculate the risk based on the risk rating color. Thus the informants proposed that a system that uses color and calculates the risk impact and probability is recommended.

b. Suggest Best Practices

Presently in making a decision, the committee always checks back and makes use of the historical data to make decision in deciding on how to treat the identified risk.

c. Stores Risk Data

The informants agreed that there is a need for a knowledge source in risk decision making, but currently the institution don't have any knowledge source that can support the committee members in making decisions in treating identified risk. Thus, the informants stated that it's better to have a knowledge source that can support the committee in making risk decisions.

d. Reuse Risk Data

Presently in the current system used by the institution, the committee only key in the risk, a more advanced technology can provide support by ranking the risk. The current technology used by the institution cannot rank the risk. However, the committee makes risk decisions based on past experience, knowledge, based on the risk scenario.

Shape Conjure

The risk decision process has been verified using the analysis of the case study, the next step is to proceed and indicate the level of acceptance of each risk decision process in mitigating risk in IT organization. This can be obtained by using an instrument that gives the same statements to each process. The informants can then indicate to what extent they agree or disagree with each statement listed in the instrument. The informants were interviewed based on the questions below;

1. The Measuring of risk impact and risk probability is important in making decisions in mitigating risk in your organisation?
2. Can best practice suggestion support the practitioners in making risk decisions in mitigating risk?
3. Should risk decision data be stored in an enterprise knowledge base?
4. Should practitioners reuse previously stored risk data in making decisions in mitigating risk?

Based on the feedback from the informants, the level of acceptance for the risk decision process can be determined. The responses helped to ascertain the gap for these statements by reviewing the answers given by informants. Thus, if the informants agree that the risk decision process in the model is similar or same to the risk decision process adopted in their organization, we can conclude that the level of acceptance of each risk decision process in mitigating risk in IT Governance is acceptable. But if all the informants disagree with any of the risk decision processes, then the level of acceptance of that risk decision process in mitigating risk in IT Governance cannot be accepted and is removed from the risk decision process. The level of acceptance of each risk decision process in mitigating risk in IT Governance can be measured by aggregating the acceptance for all statements related to each process. Thus, the level of acceptance of each risk decision process can be calculated as follows:

Level of Acceptance for each process =

$$\frac{E\ (\text{level of acceptance for each statement})}{n * Mj}$$

Where E is the summation, n is the number of process and Mj is the maximum acceptance for each statement. By using the same argument, the total acceptance between the informants for each risk decision process can thus be calculated as follows:

Total Level of Acceptance =

$$\frac{\text{E (level of acceptance for each risk decision process)}}{\text{Number of risk decision process}}$$

Phase 3 - Iteration

The purpose of this phase is to refine the risk decision process that has been developed, verified in phase 2 of the iterative triangulation. Thus, the idea can be improved; either by limiting the number of processes involved in risk decision or by reviewing the risk mitigation documents provided by the informants on how they mitigate risk in their organization. Analysis of the risk mitigation document helps to verify the existing risk decision process. Phase 4 it can be seen that the risk decision process in the risk mitigation model in Figure 4 is same with the process in the risk mitigation document from the organization in section 6.3. Therefore, the risk decision process is refined.

Phase 4 - Conclude

The evaluation process consists of applying this technique to a case study. The selected case study is the application of the developed framework. Based on the interviews conducted with the informants, the informants agreed that the risk decision process can support practitioners in mitigating risk in their organization, also the risk decision process can also assist practitioners in making decision relating to identified risk. The risk decision process provides supports in risk decisions via knowledge base. The informants were shown the framework and were explained on how to use the framework in carry out risk mitigation. The informants were finally asked to give their opinion on the framework's ability to assist in providing support to practitioners in making decision in mitigation operational and technical risk that occurs in IT organization. They agreed that the risk decision process implemented by the framework is able to support practitioners in mitigating risk and reducing the risk impact based on the risk report generated by the framework.

D. Risk Mitigation Document for Framework Evaluation

The risk mitigation document is shown in Appendix. The document comprises several sub-processes. These processes are adopted by risk assessment and mitigation team in risk decisions and mitigating risk in their organization. The first phase of the risk mitigation document is the risk mitigation purpose which states the purpose of implementing the risk mitigation. This phase is drafted by the risk assessment and mitigation team members. The next phase is to state the scope of the risk to be mitigated. In this phase, the risk assessment and mitigation team member's state which part of the organizations' system is to be mitigated. Thus, the risk assessment and mitigation team members try to narrow down the risk mitigation. Another phase is the reference documents, in which the risk assessment and mitigation team members retrieve approved risk mitigation documents from ISO such as ISO/IEC 27001:2003 which contains the information technology-security techniques, information security management system requirements and ISO/IEC 27005:2008 which comprises risk assessment guidelines for information security management and the last document utilized by the organization is the MyRAM application.

Another phase is the definition, which involves assigning explanation to all the facilities, infrastructures and terms to be used for mitigating risk. Then the risk assessment and mitigation team proceed to describe and set up risk team, by selecting suitable people for the risk mitigation process. The selected team proceeds to adopt risk assessment methodologies for ICT assets. In the organization the selected risk mitigation team members usually adopt the Malaysian Public Sector ICT Risk Assessment Methodology since 2005. Next, the risk mitigation team sets asset boundaries, by identifying the hardware, software, supporting services/accessibility, data & information flow in the systems' and people involved in the identified risk that is to be mitigated. After this phase the risk mitigation team proceeds to identify assets based on the confidentiality, integrity and availability of the asset, evaluate assets based on low, medium and high scale, assessing threats that can result to risk, assess the risk vulnerabilities, identify control measures of the identified risk, analyze the risk impact, analyze the risk possibilities, calculate the identified risk, propose risk treatments solution based on risk measurement level by making risk decision on the risk that is to be mitigated.

6. DISCUSSION AND CONCLUSION

IT organizations are handled with strategic, operational and technical risks. These risks should be mitigated. However, risk mitigation has problems with IT projects and difficulty in choosing and executing mitigation actions among project leader. Risk mitigation emphasizes taking action early in a project to prevent the occurrence of undesired events or to reduce the consequences of their occurrence. Mitigating these risks is a key factor and a major requirement in securing successful projects. Risk Mitigation provides a mechanism for practitioners to make risk decisions by providing a stepwise execution of risk process and components. The mitigation of risks aids managers to understand the mutual relationships among the enablers of risk mitigation and provides a suitable metric to quantify these risks. In risk mitigation; risk decisions are performed in order to mitigate the identified risks.

Existing risk mitigation models and frameworks lack the capacity to support risk decisions in mitigating risk. These dependencies make the technical problem of mitigating existing risks difficult. Existing risk mitigation model lacks the need for adequate data which is very important in mitigating risk and there is the difficulty of mitigating risk generally in IT organization, therefore the risk decision mitigation framework is proposed. A preliminary study was carried out; starting with the pilot study which was done utilizing the qualitative instrument (interview) to validate the instrument and data and generalize the data of risk decision in risk mitigation based on IT Governance. The pilot study was carried out using 2 organizations, where 5 informants were interviewed and the data were analyzed and reported based on people management, process management, technology management, quality management and other comments from the informants.

The risk mitigation process; risk identification, risk decision, risk treatment and risk monitoring and the risk decision components; people technology, technique, methods, procedures, management and quality of working environment obtained from the literature was verified using a qualitative study, via samples obtained from 2 case studies involving 7 informants. In the case study, open-ended interview was used to collect data. Descriptive and narrative analyze were used to analyze the interview transcript from the 2 case studies. Based on the informants' suggestion a new process was included to the existing risk mitigation process. The new process is "Risk Report". The informant added that there was the need for a process that will enable the risk mitigation team to generate monitoring report based on the identified risk. The quality of working environment was removed as one of the risk mitigation components based on the findings from the case study.

The proposed framework assists practitioners' in risk decisions and provides support in mitigating risk in IT Governance. The researcher identified the risk decision process, namely; measure risk impact and probability, suggest best practices, stores risk data and reuse risk data. The risk decision process was gotten by searching, reviewing, extracting and synthesizing each literature's on risk mitigation. The risk mitigation model comprises the risk mitigation process and the risk decision process which are influenced by the technical and operational risk components and metrics. The framework is also supported by knowledge mapping and software agents which assist in providing support to practitioners in making risk decisions. Lastly, the iterative triangulation process was used to evaluate the framework. Iterative triangulation helps to refine the risk decision process that has been developed based on case study using follow-up interview and the review of risk document from the case studies. This study has limitation which was involved and analyzed 2 case studies and it need to add more case studies for participation. Besides that, future work is aimed at implementing the risk mitigation system based on multi-software agents and knowledge mapping in the framework.

ACKNOWLEDGMENTS

We are grateful to the Ministry of Education Malaysia for the financial support, faculty of computer science and information technology, UPM for their support for this research and also to all the IT practitioners and experts who contributed to this project.

REFRENCES:

[1] ITGI.: Board Briefing on IT Governance. IT Governance Institute, USA. (2014)

[2] Saint, G. R.: Information Security Management Best Practice Based on ISO/IEC 17799. *Information Management Journal*, Vol. 39, No.1, 2005, pp. 60-66.

[3] Noraini, C. P., Bokolo, A. J., Rozi, N.H. N., Masrah, A.A. M., "A Review on Risk Mitigation of IT Governance", *Information Technology Journal*, Vol. 14, No.1, 2015, pp. 1-9.

[4] Yu, T. C., Huan, M. C., Chan, C. W., "A Study on Applying Mind Mapping to Build a Knowledge Map of the Project Risk Management of Research and Development, *2009 Fourth International Conference on Innovative Computing, Information and Control, IEEE*, 2009, pp. 30-33.

[5] Lainhart, J. W., "Why IT governance is a top management issue", *The Journal of Corporate Accounting and Finance*, Vol. 11, No.1, 2010, 33-40.

[6] Bodnar, G. H., "IT Governance. Internal Auditing", Vol. 18, No. 3, 2008, pp. 27-32.

[7] Noraini, C. P., Bokolo, A. J., "A Review on Decision Making of Risk Mitigation for Software Management", *Journal of Theoretical and Applied Information Technology*, Vol. 76, No. 3, 2015, pp. 333-341.

[8] Mihane, B. N., Albana, Q., "Improving Decision Making with Information Systems Technology – A theoretical approach", *Iliria International Review*, Vol.3, No.1, 2013, pp. 49-62.

[9] Ddembe, W., Michael, K., "Towards a Model of Decision Making for Systems Requirements Engineering Process Management", *15th International System Dynamics Conference*, Istanbul, Turkey, 2005, pp. 1-15.

[10] Khoo, Y.B., Zhou, M., Kayis, B. "An approach to rapid prototyping for a web-based risk management system", *18th World IMACS / MODSIM Congress*, Cairns, Australia, 2009, pp. 4305-4311.

[11] Kayis, B., Zhou, M., Savci, S., Khoo, Y.B., Ahmed, A., Kusumo, R., Rispler, "A., IRMAS – development of a risk management tool for collaborative multi-site, multi-partner new product development projects", *Journal of Manufacturing Technology Management*, Vol. 18, No.4, 2007, pp. 387 - 414.

[12] Ahdieh, S. K., Ow, S. H., "An innovative Model for optimizing Software Risk Mitigation Plan: A case Study", Sixth Asia Modelling Symposium IEEE Computer Society, 2012, pp. 220-224.

[13] John, D., Isaac, N., Admire, K., "Intelligent Risk Management Tools for Software Development. SACLA, *ACM*, 2009, pp. 33-40.

[14] Thamer, A. R., Shahida, S., Rosalina, A. S., "Project Management using Risk Identification Architecture Pattern (RIAP) Model: A case study on a Web-based application", *16th Asia-Pacific Software Engineering Conference*, 2009, pp. 449-456.

[15] Rajesh, S. H., Suraj, M. A., "Application of Web Based Supplier Risk Assessment for Supplier Selection", *Proceedings of the 2009 Industrial Engineering Research Conference*, 2009, pp. 2259-2264.

[16] Gabriel, J. M. O., Obara, L.C., "Management Information Systems and Corporate Decision–Making: A Literature Review", *The International Journal of Management*, Vol. 2, No.1, 2013, pp. 78-82.

[17] Cezar, V., "Effective Strategic Decision Making", *Journal of Defense Resources Management*, Vol. 1, No.1, 2011, pp. 101-106.

[18] Laudon, K. C., Laudon, K. P., Management Information System, Prentice Hall, USA. (2012)

[19] Janusz, G., Jakub, M., "Towards an integrated environment for risk management in distributed software projects, *Proceeding of 7th European Conference on Software Quality*, Helsinki, Finland, 2002, pp.1-12.

[20] Pankaj, R.S., Whiteman, L. E., Malzahn, D., "Methodology to Mitigate Supplier Risk In An Aerospace Supply Chain. *Supply Chain Management An International Journal*, Vol. 9, No.1, 2004, pp. 154-168.

[21] Jung, H. E., Lee, S.H., Lim, H.J., Chung, T. M., "Qualitative Method-Based the Effective Risk Mitigation Method in the Risk Management", *ICCSA*, 2006, pp. 239-248.

[22] Shan, L., Chen, T., Liu, Y., Zhang, J., "Evaluating and Mitigating Information Systems Development Risk through Balanced Score Card", *2009 International Symposium on Information Engineering and Electronic Commerce*, 16-17 May 2009, DOI 10.1109/IEEC.2009.28, 2009, pp. 1-5.

[23] Ahdieh, K., Hashemitaba, N., Ow, S. H., "A Novel Model for Software Risk Mitigation Plan to Improve the Fault Tolerance Process", *IJITCM*, Vol.1, No.1, 2012, pp. 38-42.

[24] Eliza, L., Dumitru, A., “A Risk Mitigation Model in SME’s Open Innovation Projects”, *Management & Marketing Challenges for the Knowledge Society*, Vol. 5, No. 2, 2013, pp. 303-328.

[25] Basit, S. Al, O. Y., Abdullah, A.: Trivial model for mitigation of risks in software development life cycle. *International Journal of the Physical Sciences*, Vol.1, No.1, 2011, pp. 2072-2082.

[26] Suresh, R. H., Egbu, C. O., “Knowledge Mapping: Concepts and Benefits for A Sustainable Urban Environment”, *20th Annual ARCOM Conference*, 2004, pp. 905-916.

[27] Mihalis, G., Michalis, L., “A multi-agent based framework for supply chain risk management”, *Journal of Purchasing and Supply Management*, Vol. 17, No.2, 2011, pp. 23-31.

[28] Fu, R., Yue, X., Song, M., Xin, Z., “An architecture of knowledge management system based on agent and ontology”, *The Journal of China Universities of Posts and Telecommunications*, Vol.15, No. 1, 2008, pp. 126-130.

[29] Pratim, D., Acar, W., “Software and human agents in Knowledge Codification”, Knowledge Management Research and Practice, Vol. 8, No.1, 2010, pp. 45-60.

[30] Noraini, C. P., Bokolo, A. J., Rozi, N.H. N., Yusmadi, Y. J., “Proposing a Model on Risk Mitigation In IT Governance”, *Proceedings of the 5th International Conference on Computing and Informatics, (ICOCI 2015)*, 11-13 August 2015, Istanbul, Turkey, pp.1-6.

[31] Ermine, J. L., Boughzala I., Tounkara, T., “Critical Knowledge Map as a Decision Tool for Knowledge Transfer Action”, *The Electronic Journal of Knowledge Management*, Vol. 4, No.1, 2006, pp. 129-140.

[32] Abdullah, M. Z., Noraini, C. P., “Measuring Communication Gap in Software Requirements Elicitation Process”, *Proceedings of the 8th WSEAS Int. Conference on Software Engineering, Parallel and Distributed Systems*, 2009, pp. 66 -71.

[33] Marianne, L. W., “Iterative Triangulation: a theory development process using existing case studies”, *Journal of Operation Management*, Vol. 16, No.1, 1998, pp. 455-469.