JOURNAL OF SOFTWARE ENGINEERING & INTELLIGENT SYSTEMS
ISSN 2518-8739
30th April 2017, Volume 2, Issue1, JSEIS, CADMEI Copyright © 2016-2017
www.jseis.org

A risk decision policy model for mitigating risk in IT organizations

[1]Bokolo Anthony Jnr, [2]Noraini Che Pa, [3]Rozi Nor Haizan Nor, [4]Yusmadi Yah Josoh
[1,2,3,4]Faculty of Computer Science and Information Technology
Universiti Putra Malaysia, 43400 UPM, Serdang, Selangor, Malaysia
Email: [1]bkanjr@gmail.com, [2]norainip@ump.edu.my, [3]rozinor@ump.edu.my, [4]yusmadi@ump.edu.my

ABSTRACT

Information Technology (IT) organizations are facing various risks such as strategic, operational and technical risks. These risks should be identified, measured and mitigated. After risks are identified, resources should be devoted to mitigate these risks. However, risk mitigation is a complicated problem especially in IT organizations. It leads to difficulty in choosing and executing mitigation actions. In risk mitigation, decision making based on the risk will be performed in order to have an efficient decision in the mitigation of identified risks. Risk mitigation in IT organizations provides a disciplinary environment for proactive decision making to measure and treat potential risk continuously. Unfortunately, present standards for risk mitigation show limitations when making decisions on how to mitigate availability risks. Existing model provides inadequate support to practitioners in making risk decision pertaining risk mitigation policies. This is due to the fact that existing approaches lack the capabilities to support practitioners, these dependencies make the technical problem of mitigating existing risks very challenging. In order to address this challenge, this research identifies the processes of risk decisions for mitigating risk in IT organizations by developing a risk decision policy model that focuses on mitigating both technical and operational risk that occurs in IT organizations.

Keywords: risk; risk decisions; decision policy; risk mitigation; IT organizations;

1. INTRODUCTION

Risk decision policy aims to direct IT organizational activities to guarantee that its performance meets the objectives set out in its strategy [1]. With effective policy, the return of IT project can be optimized to extend business strategies and goals. Risk can be normally said as something that what might go wrong in any organization. Risk is also a combination of the likelihood of an event and its effects, thus practitioners must learn to treat the possible negative effects of risk against the possible gains of its related opportunity [2].

In IT organizations, risk management is a safety consideration that defines, measures, and controls uncertain events in an attempt to reduce as many losses as possible, and to optimize IT infrastructure. Therefore, risk management involves methods to uncover potential risks, to predict losses, and to take proper action to prevent and control risk [3]. Risk mitigation has been a prime area of research since last two decades, and this area of research has received a highly overwhelming response and contribution from the researchers both in industry and academia. Risk mitigation is one of the main activities in risk decision policy. 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). It includes monitoring, tracking and evaluating risk process effectiveness throughout the utilization of IT infrastructures. The mitigation of risk provides a mechanism for practitioners to handle risk effectively by providing the step wise execution of the risk method [4]. Thus, presenting a medium to understand and express each mitigation strategy against any risk factors in IT organizations [5]. Risk mitigation is an important process to assist practitioners achieving the new business changes, future investment in information and information system [6]. Risk mitigation is sequence of phase's aims at identifying, addressing, and reducing risk before they turn out to be either threat to effective IT operation.

Poor decision making by IT practitioners in risk mitigation is due to unwillingness to rely on others for decisions, not taking ownership of decisions, conflicting priorities and unstable staff availability of decision. In risk mitigation, decision making means recognizing risks, generating alternative solutions to the risks, choosing among alternatives, and implementing the chosen alternative [7]. Nowadays risk decision policy is the key to the long-term survival of IT organizations. Each organization must be capable in making a good decision. Making good decisions often requires knowledge that can provide the decision maker with data, information and answer to questions, related to risk mitigation, without such support decisions may be based on intuitions or guesses. Decision making is important in risk mitigation to align the organization policy and procedure structure for effective decision making. According to Gabriel and Obara (2013) decision making is vital in risk mitigation and is dependent on the quality of decisions that informs its operation [8]. A suitable decision making process can

assist organizations to increase the effectiveness and incorporating improvements aimed at better understanding, improved communication and more effective management [9].

The structure of this paper is as follows; Section 2 describes the materials and methods, Section 3 describes the proposed risk decision policy model. Section 4 presents the discussion, conclusions and future works.

2. MATERIALS AND METHODS

This section briefly explores the research problem, research objectives and related work.

2.1 Research problem

One of the emerging problems in the field of risk mitigation in IT organizations is mainly due to existing approaches not being able to provide risk decision policy support to practitioners in mitigating risk. Risk decisions are performed to mitigate risks in IT organizations. Practitioners make decisions to solve operational and technical risk. However, existing models inadequately provide assistance for practitioners to make risk decisions on treating identified risk in IT organizations [10, 11]. Therefore, mitigation of risk is not properly carried out, since the risk decision policy is basically ignored by practitioners. The risk decision policy needs to be performed in order to have a proficient risk mitigation process in the mitigation of identified risks in IT organizations [10, 12, 13].

2.2 Research objectives

The objectives of this study are:

a. To identify the processes of risk mitigation in IT organization.
b. To propose a risk decision policy model for risk mitigation which focuses on both technical and operational risks in IT organization based on the first objective.

2.3 Related works

Risk mitigation mainly involves treating risk. IT organizations face several risks such as operational, technical and strategic risks. These risks should be mitigated. However, risk mitigation is very complicated, especially in IT organizations, leading to difficulty in choosing and executing mitigation actions. An effective risk mitigation plan can identify risks, thus providing useful decision support for managers [13].

Pankaj et al. (2004) presented a generic prescriptive methodology for mitigating risks in supply chain and also proposed five activities involved in risk mitigation [14]. The researcher mentioned that adapting to IT involves risk, thus organizations must identify, evaluate, rank and mitigate these risks to thrive in today's economy. The model provides a disciplined environment for proactive decision making access what might go wrong and implement strategies to deal with those risks. The model process involves risk identification, assessing risk, plan and implementing solutions, conducting failure mode and effect analysis and lastly continuous improvement.

Jung et al. (2006) suggested a qualitative method based risk mitigation method using suitable safeguards such as prevention, reduction, monitor, detection, or correction and recovery to mitigate risk with risk analysis results [15]. Appropriate and justified safeguards are identified and selected to mitigate the assessed risks to an acceptable level. The model comprises of the result of the analysis, the safeguard methods, safeguard techniques, safeguard decision and safeguard implementation.

Shan et al. (2009) developed a model for evaluating and mitigating information systems development risk using balance score card [16]. Information Systems (IS) development process risk is required to be evaluated for decision-making and the risks need to be mitigated. The model mitigates 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 BSC as to reduce IS development risks and improving development performance while guaranteeing the realization of target.

Ahdieh et al. (2012) proposes a novel model for IT and software risk mitigation plan mainly to reduce the risks consequences and their occurrence probabilities [12]. 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 IS. This model process involves creating risk mitigation plan according to obtained information from the previous project and historical data.

Eliza and Dumitru (2013) designed a risk mitigation model in small and medium enterprise (SME) [17]. The model attempts to define a comprehensive structure of internal and external risks residing in open innovation and which prevent the proper functioning of SMEs, and provide results on the factors that help to mitigate the risks

that occur in SMEs by using external knowledge to accelerate organizational and technological learning of a firm, by staying tuned with the latest risk mitigation information.

Basit et al. (2011) presented a trivial model for risk mitigation in software management that not only focuses on the identification of the risks but also provides a mechanism to mitigate the risk effectively the researchers claimed [5]. The model discusses the software risk management by providing the step-wise execution of the risk mitigation methodology by presenting an easy flowchart to express the working of each mitigation strategy against any risk. In order to mitigate the risks effectively, the researchers proposed to index the risk factors by calculating the impact and likelihood of each risk factor.

Ahdieh and Siew (2012) proposed a mitigation model of software risk management process [10]. The model makes use of risk mitigation decision which assists to create new opportunities. The identification and focusing on these opportunities increase the benefits by considering the impacts of such hidden risks. To improve the risk mitigation decisions which are the main goal of risk managers, the model uses a synthesized approach which identifies risks and opportunities together with the risk reduction activities.

3. PROPOSED RISK DECISION POLICY MODEL

The proposed risk decision policy model is based on the risk mitigation process which firstly aims to anticipate risks. Then, in the case of negative risks, it aims to prevent them from eventuating or to minimize their impact if they do. In the case of positive risks, it aims to capitalize on opportunities that present themselves. Thus, the presented model aims to treat risk in IT organizations; by involving risk decision policy of practitioners in the organization. An effective risk mitigation process is necessary to carry out these risk mitigation activities and to provide the information necessary for risk decision in IT organizations.

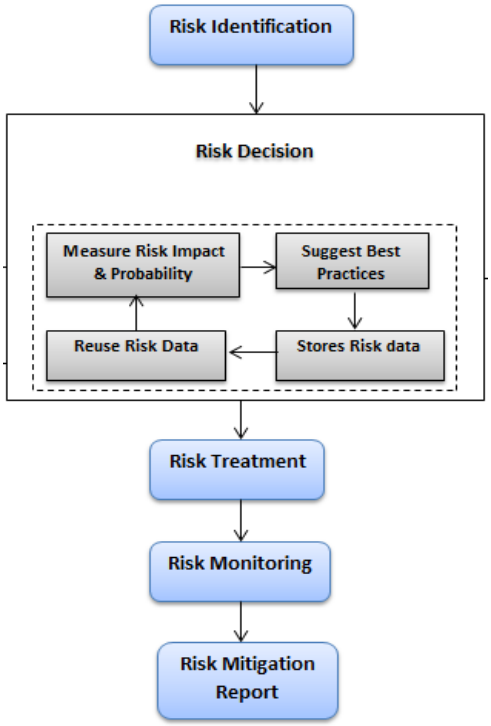

Figure. 1 Proposed risk decision policy model

Figure 1 shows the proposed model which is based on five phases. The risk mitigation process aims to assist in dealing with the risks inherent in IT organizations and thereby exercise better control over IT organizations by increasing chances of enterprise success. The risk decision comprises of four policies standards that must be carried out by practitioners in IT organization to mitigate risk that occurs in their enterprise. The model 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 as seen in Figure 1. The risk decision is the area of concentration in this research based on the research problem in Section 2.1. The risk decisions will assist in answering the research problems in this research. The model provides support to practitioners through the risk mitigation report. Thus, risk decision is the main process in the risk mitigation model where decision is carried out based on various

alternatives or solutions on how to treat the risk. The research objective 1 which aims to identify the risk mitigation process is shown in the model and described in Table 1.

3.1 Model process

Risk mitigation process to be carried out by practitioners is shown in Table 1:

Table. 1 Risk mitigation process

Process	Description
Risk identification	Risk identification is the first stage of the risk mitigation process. It is concerned with identifying the risks that could affect IT organizations negatively [13]. Risk identification may involve a team of group members who come together to brainstorm possible risks [18]. Alternatively, the practitioners may simply use their experience to identify the most probable or critical risks [19].
Risk Decision	Risk decision is the act of reaching a conclusion on the best solution to solve the risk; based on the risk magnitude and risk impact (risk measurement). Decision making is the most important phase in risk mitigation, because this is the phase the risk solution is chosen by the practitioners. However, it is also the most challenging task practitioners' face in mitigating risk. Good decision aids IT organizations to be effective. Thus, risk decision helps the decision makers to estimate the impacts of various identified risks. Risk decision has a robust comprehensive information risks mitigation policy by effectively mitigating the risks it faces. Practitioners can guard against poor decision making, using process like decision trees or risk breakdown [5, 10, 20]. Risk decision aims to deal with the risks inherent in IT Organizations and thereby exercise better control over the IT infrastructures and increase its chances of successful IT utilization.
Risk Treatment	This phase involves prioritizing the solutions of the identified risk according to their risk magnitude, defined classes of risk [19]. Risk treatment is defining an effective strategy to solve the risks associated with the various risk classes defined. In risk treatment, the practitioners' perspective is included in the treatment of IT risks by comparing various solutions to the risk, using procedures such as bench marking, cost benefit analysis and benchmark to state mission [6, 21].
Risk Monitoring	Risk monitoring aids in the checking of the risk milestones as the risk treatment is applied using process like knowledge mapping, standard risk management plan and milestone tracking. Risk monitoring is a convenient milestone for reporting, reviewing and taking action. It aims to effectively communicate hazards to practitioners and other stakeholders in order to support managerial actions [22]. Finally, the practitioners must monitor the results of the implementation to provide feedback to management for review of the selection criteria, the alternatives, and the decision [10, 23].
Risk Reporting	This phase is a new process added in this research. It is not derived from the literature but added in the model to support practitioners in generating and viewing risk mitigation activities that have been applied by the practitioners. Risk report searches the needed risk mitigation information from the enterprise knowledgebase. If the model does not find exact answers, it can seek approximate ones. The risk report phase presents the needed risk mitigation knowledge to practitioners. The risk report works with the risk monitoring phase and also displays warning message based on the state of the identified risk that is been mitigated. Thus, if the model is to be implemented as a tool the risk report will automatically informs the practitioner via email notification updates on the current state of the identified risk.

3.2 Risk decision policy process

Risk decision policy process are the sub process of risk decision to be adopted by practitioner. The outcome of risk decision process will influence practitioners risk decisions on how to mitigate identified risks. The risk decision processes are described below as:

a. Risk impact and probability measurement

Risk impact and probability measurement is the systematic process to understand the nature of risk (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 provides 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. Practitioners normally rely on their judgment and experience of previous projects and the problems that arose in them. It is not possible to make precise, numeric assessment of the probability and impact of each risk. 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 all serious risks that have more than a moderate probability of occurrence.

b. Best practice suggestion

Best practices are based on previous 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 including risk event drivers, mitigation strategies implemented, risk impact and probability constitute the database of case studies. Therefore, practitioners will be able to locate previous risk mitigation activities via a collaborative environment or a risk mitigation system.

c. Risk data storage

The knowledgebase is collation information captured from practitioners' know-how, lessons learnt (in-depth internal expertise), case studies (internal and external case-based knowledge), best practices (external benchmarking) and risk mitigation standards. The access to such a knowledge means that the model is capable of enabling the use of past successes and failures captured to mitigate risks in IT organizations.

The risk data to be stored are basically knowledge elicitation of lessons learnt is the extension of case-based studies which capture in-house past experiences in more detail. The success of a risk decision can be enhanced by considering successes and failures of previously completed risk mitigations. In other words, a success factor can be derived from historical lessons learnt; otherwise previous mistakes can be repeated leading to failures. Furthermore, the lessons learnt also help to identify location of critical risk items which are identified based on success factors from lessons learnt.

d. Reusing of risk data

The reuse of risk data in risk decision not only provides an avenue for transferring excellence from several sources into the risk mitigation process, but also serves 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 organization 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.

4. CONCLUSION AND DISCUSSION

IT organizations faced operational, technical and strategic risks that make practitioners to miss their planned schedule, time and quality. Hence, there is the need to effectively and efficiently model to mitigate such risks if practitioners want to avoid the above problems. Existing risk mitigation models in IT organizations do not provide adequate support for practitioners to make risk decisions in mitigating risk. Existing models do not provide the user with support to estimate the probability and magnitude of risks; the models also do not provide risk reduction advice. They do not cover some important aspects such as risk monitoring very well, and most of them are not easily adopted [22]. Therefore, this research developed a risk decision policy model to support practitioners in IT organizations to mitigate risk.

The developed model comprises of risk mitigation process namely risk identification, risk decision, risk treatment, risk monitoring and risk reporting. However, this research is mainly based on the risk decision similar to work carried out in [10] and [12] in their research on risk mitigation. The researchers also addressed decision making in risk mitigation, although their research was based on software development domain whereas this research study is based on IT organizations domain. The model presented is only based on the risk decision. Therefore, the developed model in this research integrated a sub process for risk decisions as seen in Figure 1.

The risk decision policies to be adopted by practitioners in IT organizations include risk impact and probability measurement, best practice suggestion, risk data storage and reusing of risk data. The developed risk

decision policy model is less complex, easy-to-use, efficient, and less time consuming. The developed model has been developed in order to tackle the limitations of the existing risk mitigation models. The model produces risk reports for risk communication and risk tracking. The model caters mainly for mitigating risk in IT organizations only. The model supports risk decision phase by providing support to practitioners in IT organization.

The developed risk decision policy model can identify, measure, treat and provide support to practitioners in mitigating perceived operational and technical risks that occur in IT organization. The core of the research is the risk decision phase that not only supports the decision-making process of the user, but also aids the risk knowledge retrieving, storing, sharing and updating process of IT organization. Thus, the model provides a systematic approach to mitigate potential risk items, thus preventing problems and failures to occur. It is designed to be used as a decision support model for decision-makers, such as practitioners, IT expert and management.

However, this research possesses some limitations, first the developed model is only suitable to IT organizations and cannot be applied to the other domain. Secondly, the model was not verified by the researcher, the model was only developed based on secondary data from existing literature. In future, the authors plan to validate the model process using qualitative study by implementing case study across three IT based organizations in Malaysia. The data will be collected using semi-structured interview from the informants. There is need to include the developed risk decision policy model to other practitioners in other domain such as educational institution and software industries. Lastly, the authors will utilize the developed model to implement a risk decision policy system to support practitioners to mitigate operational and technical risks that occur in IT organizations.

ACKNOWLEDGMENTS

We are grateful to the Faculty of Computer Science and Information Technology, Universiti Putra Malaysia in order to support this research.

REFERENCES

1. Noraini, C. P., Bokolo, A. J., Rozi, N.H. N. and Masrah, A.A. M. 2015b. A Review on Risk Mitigation of IT Governance. Information Technology Journal. 14(1): 1-9.
2. ITGI. 2008. Board Briefing on IT Governance, IT Governance Institute. Available from http://www.itgi.org [Accessed 20 February, 2016], 1-20.
3. Yu, T. C., Huan, M. C. and Chan, C. W. 2009. 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 international conference. 30-33.
4. Noraini, C. P., Bokolo, A. J., Rozi, N.H. N., and Yusmadi, Y. J. 2015a. 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 1-6.
5. Basit, S., Al, O. Y. and Abdullah, A. 2011. Trivial model for mitigation of risks in software development life cycle. International Journal of the Physical Sciences. 2072-2082.
6. Lainhart, J. W. 2010. Why IT governance is a top management issue. The Journal of Corporate Accounting and Finance 11(2): 33-40.
7. Mihane, B. N. and Albana, Q. 2013. Improving Decision Making with Information Systems Technology – A theoretical approach. Iliria International Review. 3(1): 49-62.
8. Gabriel, J. M. O. and Obara, L.C. 2013. Management Information Systems and Corporate Decision–Making: A Literature Review. The International Journal of Management. 2(1): 78-82.
9. Ddembe, W. and Michael, K. 2005. Towards a Model of Decision-Making for Systems Requirements Engineering Process Management. 15th International System Dynamics Conference. Istanbul. Turkey. 1-15.
10. Ahdieh, S. K. and Siew, O. H. 2012. An innovative Model for optimizing Software Risk Mitigation Plan: A case Study, Sixth Asia Modelling Symposium IEEE computer society. 220-224.
11. Rajesh, S. H. and Suraj, M. A. 2009. Application of Web Based Supplier Risk Assessment for Supplier Selection. Proceedings of the 2009 Industrial Engineering Research Conference. 2259-2264.
12. Ahdieh, K., Hashemitaba, N. and Ow, S. H. 2012. A Novel Model for Software Risk Mitigation Plan to Improve the Fault Tolerance Process. IJITCM, 38-42.
13. Junchao, X., Leon, J. O., Jie, C., Qing, W. and Mingshu, Li. 2013. Search Based Risk Mitigation Planning in Project Portfolio Management. International Conference on Small Science (ICSS). 146-155.

14. Pankaj, R.S., Whiteman, L. E. and Malzahn, D. 2004. Methodology to mitigate supplier risk in an aerospace supply chain. Supply chain management an international journal, 9(1): 154-168.
15. Jung, H. E., Lee, S.H., Lim, H.J. and Chung, T. M. 2006. Qualitative Method-Based the Effective Risk Mitigation Method in the Risk Management. ICCSA. 239 – 248.
16. Shan, L., Chen, T., Liu Y. and Zhang, J. 2009. Evaluating and Mitigating Information Systems Development Risk through Balanced Score Card, 2009 International Symposium on Information Engineering and Electronic Commerce, 16th -17th May. 111-115.
17. Eliza, L. and Dumitru, A. 2013. A Risk Mitigation Model in SME's Open Innovation Projects. Management & Marketing Challenges for the Knowledge Society. 303-328.
18. Vu, T. and Liu, D. B. 2007. A Risk-Mitigating Model for the Development of Reliable and Maintainable Large-Scale Commercial-Off-The-Shelf Integrated Software Systems. IEEE Proceedings Annual Reliability and Maintainability Symposium. 361–367.
19. Davide, A., Dulmin, R. and Mininno, V. 2012. Risk Assessment in ERP projects. Information Systems. 37(1): 183-199.
20. Mohd, N. F., Banwet, D.K. and Shankar, R. 2007. Information risks management in supply chains: an assessment and mitigation framework. Journal of Enterprise Information Management. 20(1): 677-699.
21. Lientz, B. P. and Larssen, L. 2006. Risk Management for IT projects: how to deal with over 150 issues and risks. Risk management practices. 1(1): 1-15.
22. Khoo, Y.B., Zhou, M. and Kayis, B. 2009. An approach to rapid prototyping for a web-based risk management system, 18th World IMACS / MODSIM Congress. Cairns Australia. 4305-4311.
23. Emmanuele, Z., Bolzoni, D., Etalle, S. and Salvato, M. 2009. Model-Based Mitigation of Availability Risks. IEEE international Conference.75-83.

AUTHORS PROFILE

Bokolo Anthony Jnr. completed his MSc in Computer Science from Universiti Putra Malaysia in 2015. His research interest are in information systems, sustainability, software management and knowledge management. He is currently a research fellow at Universiti Malaysia Pahang.

Dr. Noraini Che Pa obtained her Ph.D. degree in Computer Science from the Universiti Kebangsaan Malaysia. Currently, she is a senior lecturer in the department of Software engineering and Information System, Faculty of Computer System and Information Technology, Universiti Putra Malaysia. Her research interest includes requirements engineering, information system, knowledge management and management information system.

Dr. Rozi Nor Haizan Nor has acquired her doctorate from University of Technology Malaysia (UTM) in Computer Science. She is currently working as a senior lecturer in the department of Software Engineering and Information System in Faculty of Computer Science and Information Technology (FSKTM), Universiti Putra Malaysia (UPM) Selangor, Malaysia. Her expertise is in the area of Information Systems, ICT services, ICT service quality and ICT Governance.

Dr. Yusmadi Yah Josoh received her PhD from the National University of Malaysia, UKM in 2008. She is currently a senior lecturer at the Department of Software Engineering and Information Systems, Universiti Putra Malaysia. Her current research interests include Management Information System, Information System, Information Technology Strategic Planning and Software Project Management.