PROPOSING A MODEL ON RISK MITIGATION IN IT GOVERNANCE

Noraini Che Pa[1], Bokolo A. J.[2], Rozi Nor Haizan Nor[3] and Yusmadi Yah Jusoh[4]

[1]*Universiti Putra Malaysia, (UPM), Serdang Malaysia, norainip@upm.edu.my*
[2]*Universiti Putra Malaysia, (UPM), Serdang Malaysia, result4real@yahoo.com*
[3]*Universiti Putra Malaysia, (UPM), Serdang Malaysia, rozinor@upm.edu.my*
[4]*Universiti Putra Malaysia, (UPM), Serdang Malaysia, yusmadi@upm.edu.my*

ABSTRACT. Risk mitigation is the core process in IT Governance. Due to the fact that application of IT Governance systems may sustain risks, organizations use risk mitigation to solve risks within IT systems and provide sufficient means to treat these risks. Risk mitigation is necessary to ensure a successful IT Governance implementation. The risk mitigation process comprises of risk identification, risk decision, risk treatment and risk monitoring. The aim of this paper is to present the new risk mitigation models' components and metrics for measuring the risk in IT Governance.

Keywords: metrics, components, risk mitigation, IT governance

INTRODUCTION

IT governance aims to direct IT endeavors to guarantee that organisations performance meets the objectives set out in its strategy. With effective governance, the return of IT venture can be optimized to extend business strategies and goal (ITGI, 2008). Risks are events that negatively impact the organization's ability to achieve their goals as far as the probability of their occurrence and the related consequences are concerned. Risk can, however, be treated in accordance with proper mitigation practices and procedures (Abdullahi and Shuib, 2011). Mitigating risks means identifying and quantifying these risks so that mitigation actions may be planned and developed to treat the risks (Wei-Ming, 2010). Risk mitigation can protect organizations and maintain their abilities to carry out missions and activities against risk as well as helping to implement mitigation actions that are actually needed (Chi and Wan, 2012). Risk mitigation also includes determining risk reducing measures (Sandip and Jigish, 2010). According to Sneh and Ujjawal (2011) risk mitigation is used to minimizing the effect of the risk. Risk mitigation consist of the various activities such as risk planning control measures, implementing risk control measures, monitoring the risk, controlling the risk, learning on risk (Sneh and Ujjawal, 2011). Bharat et al. (2012) also contributed by stating that risk mitigation is an action that help IT practitioners to understand and solve the risk (Bharat et al., 2012).

These particularly results in a gap in mitigating risk. To mitigate risk in IT Governance, three dimensions of risk are considered; operational risk, technical risk and strategic risk. The operational risks threaten the IT Governance plan. Technical Risk threatens the quality and timeliness of IT products to be produced. Strategic risk affects the development of product to be developed and often threaten the whole IT people and system. Despite many scholars and IT practitioners recognizing risk mitigation processes in IT Governance insufficient attention

has been paid by researchers to select a suitable risk mitigation model. This paper attempts to address this limitation and the gap in the current literature and provide a new risk mitigation model to give researchers and IT practitioners an insight on the current level of risk mitigation in IT Governance by presenting the needed components and their respective metrics for mitigating risk in IT Governance. This paper is organized as follows. In the next section we present the related work. In the third section we present the risk model showing the risk components and metrics. Finally we concluded the work with the conclusion section.

RELATED RESEARCH

Risk mitigation may be implemented through the use of wide variety of risk mitigation models, process or applications that provides quantitative or qualitative measurement of the risks involved (Abdullahi and Shuib, 2011). Ahdieh and Siew (2012b); proposed a model for software risk mitigation plan involves creating risk mitigation plan, and driving the actual risks. Their model reduces the risk consequences and their occurrence probabilities. Identifies effective factors in fault tolerance, the risks consequences, and presenting solutions to reduce the risks. Components are people, environment, organisation and the metrics are Commitment, Availability, Cooperation, Effectiveness, Stability, Flexibility, Cost, Dependability, Capability, Suitability and Integration. Mohd et al. (2007) presented a model to mitigate IT risk and provides managers and decision makers with an opportunity. Components are People, Technology, procedure, policy, decision makers and the metrics are Capacities, Collaboration Modularity, Transferability, Clarity, Effectiveness, Extensibility, Susceptibility, Consistency, Agility, Interoperability, Dependability and Predictability.

Sailesh et al. (2008) proposed a risk mitigation model for a robust design process that helps mitigate the risks associated with the development in IT environment. Components comprises of Process, Staff, Technology, process and the metrics are Commitment, Collaboration, Coordination, Reliability, Effectiveness, liability, Vulnerability, Compatibility, Consistency, Viability and Acceptability. Vu Tran et al. (2007) developed a risk mitigating model for integrated software systems for effectively identifying and address these potential technical risks. Components are People Guidelines, Infrastructure, process and the metrics are Trust, Capacities, Resource Availability, Reliability, Time, Capability, Efficiency, Performance, Security, Data Integrity, Consequences, Consistency, Agility, Modularity and Operability. Ahdieh and Siew (2012a) designed a software risk mitigation process model that facilitates the development of comprehensive risk mitigation plan by focusing on the unseen risks and opportunities accompanying with the risk mitigation decisions. Components are team members, process, technique and the metrics are Transferability, Acceptability, Extensibility, Correctness, Clarity, Predictability, Dependability, Time and Trust. Jubchao et al. (2013) designed a Search Based risk mitigation planning Model for solving the Problem of mitigating risk in software projects thus providing useful decision support for managers. Identified components include people, procedure, methods, technology and guidelines. Metrics includes Expenses, Security, Data Integrity, Capabilities, Complexity, Simplicity, Performance, Reliability Capacities, Resource Availability, Resource Useage, Mentality, Team Behavior and Efficiency.

METRICS FOR RISK MITIGATION

An effective risk mitigation model can assists in determining appropriate risk treatment procedures to meet the needs of the organizations. It's critical to mitigate risk in IT Governance, therefore we propose a new risk mitigation model showing the models components and

metrics as shown in Figure 1 and Table 1. The model consists of six components such as people, management, technology, method, techniques and risk mitigation and 35 metrics in total.

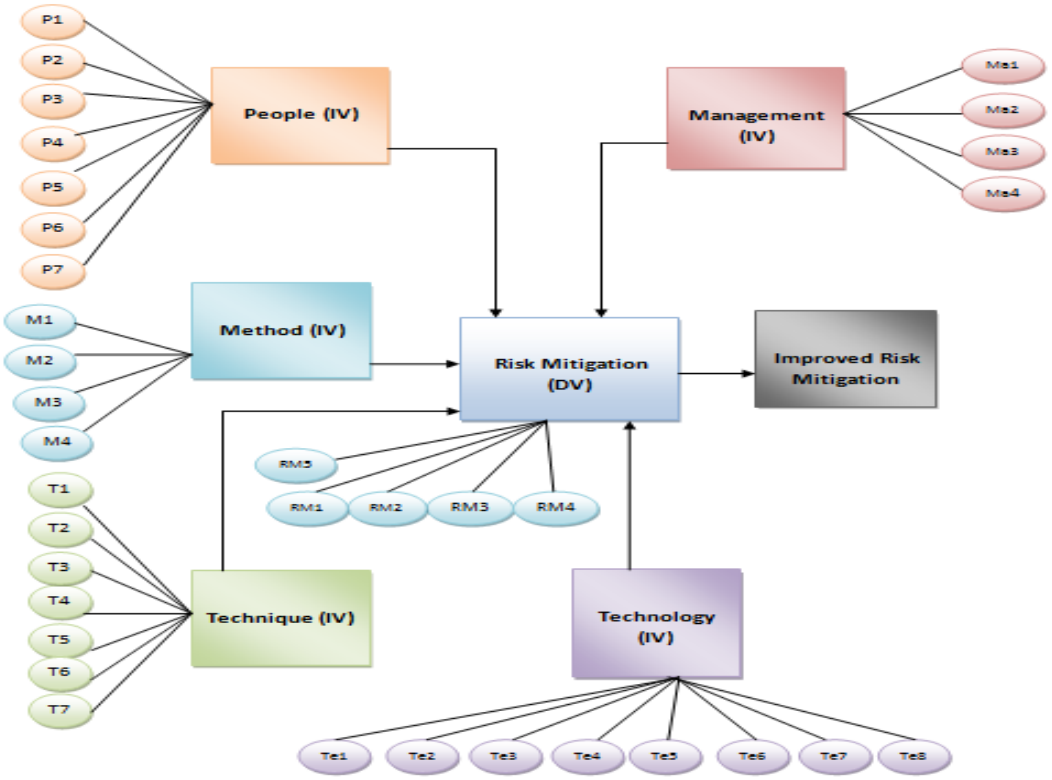

Figure 1. A Model for Risk Mitigation in IT Governance

IV are the independent variable and DV are the dependent variable, the IV (people, method, technique, technology, management influences the DV (Risk mitigation), thus the arrows point from the IV to the DV. The IV's are independent components implemented in IT organisation to carry out the DV which is the existing risk mitigation process or system.

People. This component comprises of the staffs or team members who carry out risk mitigation in the organisation (Ahdieh and Siew, 2012ab; Mohd et al., 2007)**.** People are the strength of any risk mitigation success in IT Governance. People are also a key determinant of risk since risk mitigation is the fundamental driver to sustainable success in any organisation.

Technology. This component involves the technologies (application, hardware, software networks communication) that are deployed to carter for mitigation risk (Sailesh et al., 2008; Mohd et al., 2007)**.**

Technique. This component states the process employed to mitigate risk in IT Governance, the processes are carried out by the team members or staffs in the organisation. Involves techniques that assist in risk mitigation such as spread sheets, focus group, discussions, scenario analysis, brainstorming, lessons learnt, checklist, risk breakdown, inductive reasoning, SWOT analysis, team meeting, worksheet lists (Sailesh et al., 2008; Ahdieh and Siew, 2012ab; Mohd et al., 2007; Vu and Liu, 2007).

Management. This component comprises of the stakeholders that produce guidelines and make decision involving the mitigation of risk in the organisation (Pankaj et al., 2004; Mohd et al., 2007).

Method. This component highlights the approaches used to mitigate risk in IT Governance (Sailesh et al., 2008). Involves either qualitative or quantitative methods such as Interview, questionnaire, workshops, survey used for risk mitigation.

Risk Mitigation. This is the dependent variable that relies on the other variables; this is the current risk mitigation process or software (Ahdieh and Siew, 2012a; Shan et al., 2009).

Table 1. Component and Metrics of Risk Mitigation Model

Components	Metrics
People	P1=Trust [Trust between team members; help them reach their ability to mitigate risk]
	P2=Supportability[Team members available to supports each other to mitigate risk in the organization]
	P3=Commitment[Interest and concerned of team members to mitigate risk in the organisations]
	P4=Collaboration[Team members' willing to involve in the mitigation process]
	P5=Cooperation[Team members' work together to help each other in mitigating risk]
	P6=Capabilities[The talent, ability and potential of team members to achieve performance goal in risk mitigation]
	P7=Communication[Interaction among team members in mitigating risk]
Technology	P1=Interoperability[Ability to work with other systems using different platform]
	P2=Efficiency[Ability to offer proper support when mitigating risk]
	P3=Performance[The usefulness of the risk mitigation results provided by the technology]
	P4=Security[The technology protects the data and resources related to risk mitigation]
	P5=Data Integrity[The technology protects against the altering of the data relating risk mitigation]
	P6=Reliability[Ability to maintain a specified level of performance, when used under specified conditions]
	P7=Responsiveness[Ability to react quickly when performing activities and complete assigned tasks within a given time]
	P8=Functionality[Ability of the technology to provide the required services to aid risk mitigation]
Method	M1=Suitability[The method is suitable for mitigating risk]
	M2=Opportunities[The benefits the risk mitigation method provides]
	M3=Consequence[The method provides disadvantages or negative effects]
	M4=Consistency[The method results are always at the same level or standard]
Technique	T1=Time[Duration or how long it takes for a specific activity to be carried out in supporting risk mitigating]
	T2=Cost[The monetary value spent when applying a technique for mitigating risk]
	T3=Dependability[If the technique depends of other technique to provide its specified services when mitigating risk]
	T4=Predictability[The technique that produce ability to predict result of risk mitigation]
	T5=Flexibility[Ability for the technique to adapt to possible or future changes in its approach for mitigating risk]

Management	T6=Complexity[Ability of the technique to be complex or simple in supporting risk mitigation]
	T7=Effectiveness[The technique response time and availability in mitigating risk] Ma1=Policy[Guidelines, rules, regulations, laws, principles, or directions for team members in mitigating risk]
	Ma2=Awareness[Decisions makers' knowledge about risk from past events, or based on information or experience]
	Ma3=Resources[Available people, materials, equipment, finance, knowledge and time for risk mitigation]
	Ma4=Incentives[How much pay the management allocates to team members to boost their performance]
Risk mitigation	RM1=Redundancy[The duplication of critical process with the intention of increasing reliability in risk mitigation]
	RM2=Competency[The ability of the risk mitigation software or process to mitigate risk successfully, efficiently or properly]
	RM3=Maintainability[How easy to add new functions to the existing risk mitigation process without causing any issues]
	RM4=Adaptability[Ability of the risk mitigation process to change or be changed to work better in some cases]
	RM5=Integrity[Ability of the risk mitigation process to work alongside with other system in mitigating risk]

CONCLUSION

Risk mitigation is important in IT Governance because it assist in solving risk. The goal of model is to mitigate mainly operational and technical risk. Risk mitigation includes risk identification, risk decision, risk treatment, risk monitoring. The components and their metrics are important for mitigating risk in IT Governance. By using the model IT practitioners and IT managers could justify resource allocation. Also, the metrics could also be used by organisation for risk control. The model provides a beneficial components, metrics and knowledge for the mitigation of risk in IT Governance. The model may be valuable for the organizational business and academic circles to follow and refer. It is hoped that the model can offer a guideline for information on risk mitigation suitable for the enterprise and can be used as a reference for internal auditors and IT practitioner. Future publications will be to publish the validation results of the model by survey conducted among IT experts.

ACKNOWLEDGMENTS

We are grateful for the Ministry of Education Malaysia financial support for the project.

REFERENCES

Abdullahi, Mohamud, S., & Basri, S. (2011). A Study on Risk Assessment for Small and Medium Software Development Projects: *International Journal on New Computer Architectures and Their Applications (IJNCAA)*, 1(2), 325-335.

Ahdieh, S. K.., & Ow, S. H. (2012). A Novel Model for Software Risk Mitigation Plan to Improve the Fault Tolerance Process. *IJITCM*, 38-42 Retrieved from: http://umexpert.um.edu.my/file/publication/00001317_88617.pdf.

Ahdieh, S. K.., & Ow, S. H. (2012). An innovative Model for optimizing Software Risk Mitigation Plan: A Case Study. *Sixth Asia Modelling Symposium IEEE computer society*, 220-224.

Bharat, S., Kapil, D. S, & Subhash, C. (2012). A New Model for Software Risk Management. *Int.J.Computer Technology & Applications*, 3(3), 953-956.

Chi-Chun, Lo., & Wan-Jia, C. (2012). A hybrid information security risk assessment procedure considering interdependences between controls. *Expert Systems with Applications*, 39, 247–257. doi:10.1016/j.eswa.2011.07.015

ITGI. (2008). *Board Briefing on IT Governance*. IT Governance Institute: Retrieved from http://www.itgi.org

Junchao, X., Osterweil, L. J, Chen, J, Wang, Q & Mingshu Li. (2013). Search Based Risk Mitigation Planning in Project Portfolio Management. *ICSSP'13*, 146-155.

Mohd, N. F., D.K. Banwet & Shankar, R. (2007). Information risks management in supply chains: an assessment and mitigation framework. *Journal of Enterprise Information Management*. 1741-0398 DOI 10.1108/17410390710830727

Pankaj, R.S., Whiteman, L. E. & Malzahn, D. (2004). Methodology to mitigate supplier risk in an aerospace supply chain. *Supply Chain Management an International Journal*, 154-168. DOI 10.1108/13598540410527051

Sailesh, N., Eshahawil T., Gindyl. N, Tang. Y. K., Stoyanov. S, Ridout. S, & Bailey, C. (2008). Risk Mitigation Framework for a Robust Design Process. *2nd Electronics System integration technology conference Greenwich*, UK.12-13 February 2008. 1075-1080

Sandip, P., & Jigish, Z. (2010). A Risk-Assessment Model for Cyber Attacks on Information Systems. *Journal of Computers*, 5(3), doi:10.4304/jcp.5.3.352-359

Shan, L., Chen. T, Liu. Y, & Zhang, J. (2009). Evaluating and Mitigating Information Systems Development Risk through Balanced Score Card. *International Symposium on Information Engineering and Electronic Commerce*, DOI 10.1109/IEEC.2009.28

Vu, T., & 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.