http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet

Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 14 (1): 1-9, 2015
ISSN 1812-5638
© 2015 Asian Network for Scientific Information

ansinet
Asian Network for Scientific Information

REVIEW ARTICLE OPEN ACCESS

DOI: 10.3923/itj.2015.1.9

A Review on Risk Mitigation of IT Governance

Noraini ChePa, Bokolo Anthony Jnr, Rozi Nor Haizan Nor and Masrah Azrifah Azmi Murad
Faculty of Computer Science and Information Technology, University Putra Malaysia (UPM), Serdang, Selangor, 43400, Malaysia

ARTICLE INFO
Article History:
Received: October 13, 2014
Accepted: April 30, 2015

Corresponding Author:
Noraini ChePa
Faculty of Computer Science and Information Technology,
University Putra Malaysia (UPM),
Serdang, Selangor, 43400, Malaysia

ABSTRACT

Risk Mitigation (RM) is one of the important activities in risk management of IT governance. In IT governance project, IT risk mitigation emphasizes taking action early in a project to prevent the occurrence of undesired events or to reduce the consequences of their occurrence. The essential of RM in IT governance enables enterprise achieving "the new business changes, reduces IT project risks and future investment in IT governance projects. To get clear understanding in regards risk mitigation based on IT governance context, many relevant studies have been reviewed from different issues and aspects. The purpose of this study is to investigate related RM frameworks, models, processes, stakeholder involves and other issues based on a Systematic Literature Review (SLR) approach. This study presents the results of the systematic literature reviews on an evident of the RM in IT governance and it issues that need to be catered in the future. The finding of this review indicates that RM requires appropriate consideration to systematically reviewed on it numerous limitations, issues and current implementation.

Key words: Risk mitigation, risk management, IT governance, systematic literature review

INTRODUCTION

Risk is considered as possibility of occurrence or event or condition that will have a positive or negative effect on a project objective. According to Sommerville (2011) there are three categories of risks: Projects risks, product risks and business risks. In order to adapt against business changes, emergence risks and future investment, the organisations must learn to solidity the potential effects of risk alongside its related opportunity (ITGI, 2005). There are many types of risks related to IT governance such as strategic, operational, technical and IT service delivery and enterprise risk. The strategic risks are contributing lack of investment, different understanding of the business process, less support by management and unresolved conflicts between business and IT management. Kumsuprom *et al*. (2008) stated that the adoption of IT application has also brought organizations' risks related to IT such as strategic risk, financial risk, operational risk and technological risk.

Risk mitigation is in place to ensure that risks have been adequately resolved in the organization. Effective risk mitigation makes it easier to cope with problem and to ensure that these do no lead to unacceptable situation through identifying, making decision, treatment and monitoring the impact of risks. In order to minimize and control these risks successfully, IT risk mitigation policies and strategies have been developed and implemented in organizations. Risk mitigation emphasizes taking action early in a project to prevent the occurrence of undesired events or to reduce the consequences of their occurrence. Risk mitigation mainly involves transferring, avoiding, controlling and even accepting risk. According to Xiao *et al*. (2013), risk mitigation focuses primarily on actions for estimating and planning the schedule, resources and funding.

Risk treatment is defining an effective strategy to solve the risks associated with the various risk classes defined. Risk control aims to deal with the risks inherent in a project and thereby exercise better control over the project and increase its chances of success. Furthermore, monitoring and review is a convenient milestone for reporting, reviewing and taking action. Communication and consulting aims to effectively communicate hazards to project managers and other stakeholders in order to support managerial actions.

Risk mitigation is one of the main and important activities in IT governance. In practice, IT Governance supports the business, adding plus value through IT component and IT risks minimisation. IT governance is a very important issue at present as an integral component of any corporation or organization. The purpose of IT governance is to direct IT endeavours to ensure that IT's performance meets the objectives set out in its strategy (Lin *et al*., 2011). Risk mitigation includes risk monitoring and enhances identified risk tracking, evaluating risk. IT governance is mainly focused on the area of IT strategic alignment, IT resource management, risk management, performance measurement and IT value delivery (ITGI., 2008). An effective risk mitigation model can identified, thus providing useful decision support for managers (Xiao *et al*., 2013).

In practice IT Governance supports the business, adding plus value through IT component and IT risks minimisation. In order to achieve such purposes IT Governance should cover five principal domains; IT Strategic alignment, Value delivery, Risk management, Resource management, Performance measurement (ITGI., 2001; Bodnar, 2003) (Fig. 1).

The overall objective of this work is to carry out a comprehensive review and synthesis of the current research, practices, issues and challenges of RM based on the prior work done by many researchers. Though, all studies agree on the importance of RM but there is no consensus on the framework, model and processes involved in their implementation. For this reason this paper aims to do research of RM from 2005 until 2014 including their framework, models, processes, advantages, challenges and limitations.

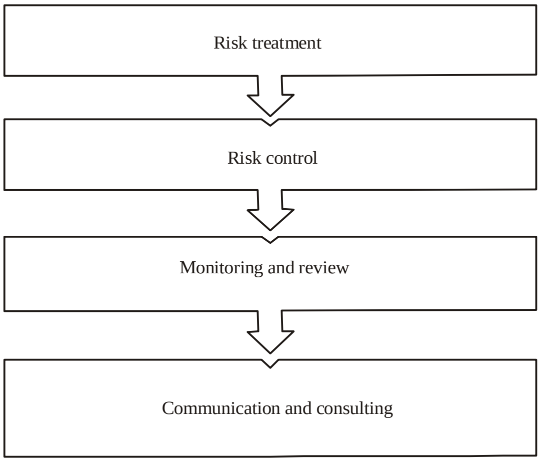

Fig. 1: Risk mitigation process (Aloini *et al*., 2012)

MATERIALS AND METHODS

This section explores the materials and methods involved for collecting and analyzing existing research work. SLR provides methodological advantages and applicability to research questions. The SLR comprises three main phases namely planning, conducting and reporting (Brereton *et al*., 2007). These main phases are illustrated in Fig. 2.

Planning the review: The study started with identifying the needs for a literature review, formulating the review research questions and review protocol. The review was performed by defining the initial protocol. The actual gathering process was performed and the results were evaluated using subsequent harvesting steps and adapted the search strategy. Data was extracted from the selected studies, finally the data was synthesized and analyzed.

Our review approach to analyzing published studies enables us to identify reliably where the literature presents the different practices developed to carry out this task. We summarized this evidence in order to investigate Risk mitigation in IT Governance. We conduct this SLR by following the guidelines for performing SLR as proposed by Kitchenham and Charters (2007). We looked at the literature to answer these research questions:

Question 1: What is the practice of Risk mitigation?
Question 2: What are the existing frameworks and models for Risk mitigation?

A review protocol is essential to any systematic literature review. Driven by the research questions, the protocol defines inclusion/exclusion criteria to select primary studies (Table 1).

Search process: A review protocol was designed to guide the search process based on the SLR guidelines (Kitchenham and Charters, 2007). Relevant papers are retrieved automatically from the databases as well as manually from target journals, conferences and workshops as a supplementary source to the

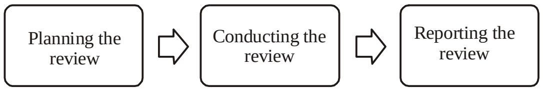

Fig. 2: SLR research phases

Table 1: Inclusion and exclusion criteria

Inclusion criteria	Exclusion criteria
Study concerns IT risk, risk Mitigation, risk management and IT Governance	The patterns are not described in detail, or a structured template is lacking
Were published in, or submitted to, a conference or journal or were technical reports or book chapters and is published between 2005 and 2014	A newer study exists that documents the same patterns
The abstract and content are written in English	The paper concerns a review or evaluation of existing patterns for Risk mitigation
Reported SLRs or meta-analyses in Risk mitigation and IT Governance	

Table 2: Data sources

Sources	Name
Journals	International Journal of Information Technology and Computer Science (IJITCS)
	Journal of Enterprise Information Management
	Journal of Inter Disciplinary Research
	Supply Chain Management an international Journal
	The Journal of International Social Research
	Information and Software Technology (56) 2014
	International Journal of the Physical Sciences Vol. 6 (8), 2011
	International Journal of Information Technology and Computer Science (IJITCS)
	Journal of Enterprise Information Management
Conference	2012 Sixth Asia Modelling Symposium
	1997 Proceedings Annual Reliability and Maintainability Symposium
	2009 International Symposium on Information Engineering and Electronic Commerce
	Proceedings of the 2005 The Fifth International Conference on Computer and Information Technology (CIT'05)
	2012 Fourth International Conference on Computational Intelligence, Modelling and Simulation
	2009 16th Asia-Pacific Software Engineering Conference
Workshops	2011 Sixth IEEE International Conference on Global Software Engineering Workshops
	Management and Marketing Challenges for the Knowledge Society
	Management Information Systems

database search. In order to make this SLR credible, the studies without any validation were excluded according to the evidence levels. In the end, the papers are finally selected to be further analyzed in this SRL. The period of published studies is stated from 2005 to 2014.

Data sources: In order to locate important material, additional searches were performed directly on key conference proceedings, journals and authors (Table 2). The electronic databases included in this SLR includes IEEE Xplore, ACM Digital library, ScienceDirect, SpringerLink, Wiley InterScience and Google Scholar. The sources includes journal, conference proceeding and workshops.

Search terms: This section defines the databases search terms based on the SLR guidelines. A search string was constructed using relevant terms based on the research questions. The following Boolean search strings were used: “Risk mitigation” or “Risk management” or “Knowledge risk” or “risk quantitative” or “risk qualitative” or “IT governance” Before we selecting the papers to be used for the SLR we check for repeating in studies to ensure there is no duplication; for example if the same study is published in two different journals with different first authors, only one study would be included in the review; usually the most comprehensive study or the most recent study. Where we need to make this choice, we include the most comprehensive study or the most recent study.

RESULTS AND DISCUSSION

A total of 25 studies discuss the Risk mitigation methods in IT Governance. Citations for the papers and other relevant papers are included in the reference for further reading. The inspected publications were classified according to the applied research method. Figure 3 shows that out of the 25 studies, 60% are empirical, 30% theoretical and 10% are either reviews of the literature or secondary studies, where empirical work is re-examined. Out of the 15 studies that are empirically based, 70% are online survey, 15% questionnaire, 8% interview and 7% are others. Figure 4 shows how these data collection methods of the empirical studies.

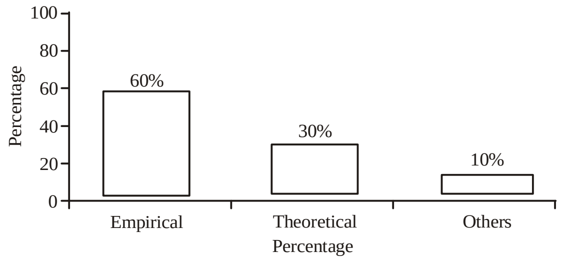

Fig. 3: Research method in paper studies

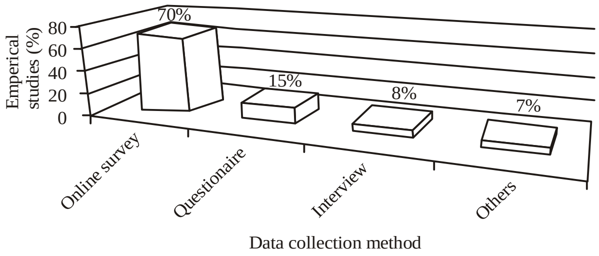

Fig. 4: Data collection methods used in the empirical studies

The reviewed papers were published between 2005 and 2014. Figure 5 shows that more papers were published in 2005 in relation to our research ‘Risk mitigation in IT Governance.

Risk mitigation process: Risk mitigation mainly involves transferring, avoiding, controlling and even accepting risk. The risks can be mitigated in quite a few different ways, each of which may require different resources at different times but for selecting the best mitigation action is not an easy task. However, the high rate of failures in IT projects shows the

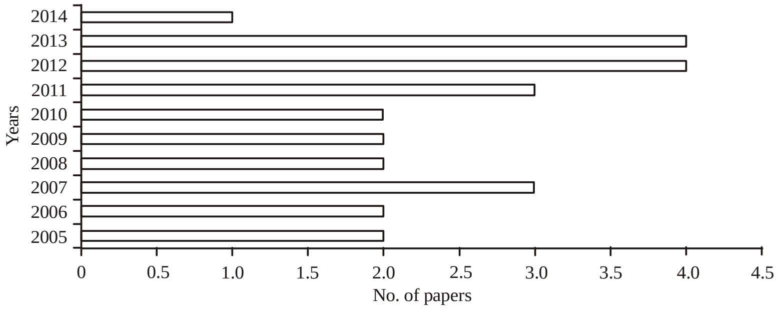

Fig. 5: Number of papers included in the review by 1-year intervals

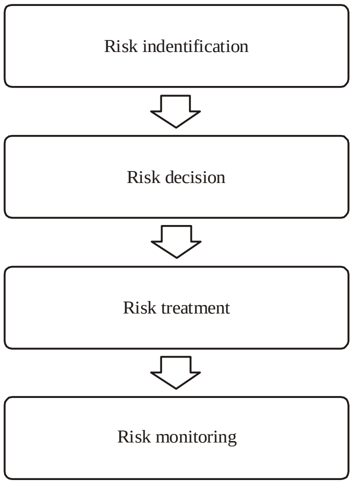

Fig. 6: Risk mitigation components

unsuccessfulness of the activities of risk mitigation (Fig. 6). The reason is the existence of hidden and unseen threats and risks in the process which are ignored in most of the models (Khatavakhotan *et al*., 2012). Researches show that risks can be mitigated by stabilizing the requirements, designs and implementations (Khatavakhotan *et al*., 2012). Besides that, developing an integrated mitigation plan is a core responsibility of a risk manager.

Zambon *et al*. (2007) pointed out that risk mitigation focuses on identifying strategic and tactical approaches to minimize the negative impacts of the identified risks to the systems overall functionality, reliability, performance and maintainability. Nowadays the process of assessing and mitigating availability related risks depends very much on the human expertise. The goal of Risk mitigation is to bring down the estimated downtime cost by applying a set of countermeasures which can be either technical or organizational (Zambon *et al*., 2007). Risk mitigation components are risk identification, risk decision, risk treatment and risk monitoring.

In risk identification potential risks are determined by Risk analysts, IT Manager, Project team and System Analyst Senior Engineer by using process such as risk rating, screening, examination of risk drivers and assumption risk analysis. Risk decision helps the decision makers to estimate the impacts of various risks and have robust comprehensive information risks mitigation policy by effectively mitigating the risks it faces, organisations can guard against poor decision making, (Faisal *et al*., 2007; Shahzad *et al*., 2011) using process like decision tress or risk breakdown. In risk treatment, the management perspective is included in the treatment of IT risks by comparing various solution to the risk (Lainhart, 2000; Lientz and Larssen, 2006), using process such as Bench marking, cost benefit analysis and benchmark to state mission and 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. Another standard that has been developed is the ISO/IEC 17799 which uses a bottom-up approach to IT risk mitigation. A representative of risk mitigation components is the ISO/IEC 17799 standard for effective IT risk mitigation. The ISO/IEC 17799 standard focuses on a detailed technical solution to risk mitigation (Saint-Germain, 2005; Von Solms, 2005).

This standard represents a bottom-up approach which explains detail technical processes coping with IT risk mitigation. The ISO/IEC 17799 standard provides organizations with the specific details on how the ISO/IEC 17799 standard can be used for controlling, preventing and mitigating IT risks. This approach is however often criticized due to its over emphasis on the technical implementation of risk mitigation (Karabacak and Sogukpinar, 2006; Mellado and Rosado, 2007; Von Solms, 2005).

Risk mitigation techniques: Two distinct techniques have been proposed to explain risk mitigation: quantitative and qualitative. Quantitative technique use measurable, objective data to determine asset value, probability of loss and associated risk (s). The goal is to try to calculate objective numeric values for each of the components gathered during the risk mitigation and cost-benefit analysis. Qualitative technique use a relative measure of risk or asset value based on ranking or separation into descriptive categories such as low, medium, high; not important, important, very important; or on a scale from 1-10. A qualitative technique assesses the impact and likelihood of the identified risks in a rapid and cost-effective manner.

Table 3: Quantitative techniques for risk mitigation

Categories	Description
Bayesian method	Bayesian models have developed procedures to revise probability by changing the initial values based on experimental results
Belief functions method	This method allows combining evidence sources and arrives at a degree of belief
Decision making matrix	A decision making matrix is a graphical tool that combines information such us the chance of occurrence of an event and the consequences of the event for quantifying risk as the product of both concepts
Decision tree analysis	Decision tree analysis helps in forming a balanced picture of the risks and rewards associated with each possible course of action
Expected Monetary Value (EMV)	Expected monetary value analysis is a statistical concept that calculates the average out come when the future includes scenarios that may or may not happen
Failure Mode and Effect Analysis (FEMA)	Failure mode and effect analysis is a quantitative tool that consists of evaluating potential process failures, evaluates risk priorities and helps determine and assess the impact of those causes
Fault Tree Analysis	It is a graphic model of the pathways within a system that can lead to a foreseeable and undesirable loss event
(FTA) Interviewing	Interviewing techniques are employed to assess probabilities and the impact of achieving specific objectives based on input from relevant stakeholders and subject matter experts
Monte carlo method	Monte Carlo method is the application of laws of probability and statistics to natural and physical sciences. It is a method of investigating the effect on a strategy of the main risks as simultaneous and non-linear interaction
Program Evaluation and Review Technique (PERT)	Program Evaluation and Review Technique is a useful tool for scheduling, organizing and coordinating different tasks in a project
Probability distributions	Probability distributions are used to graphically illustrate risk probability, representing the probability density functions
Scenario analysis	Scenario analysis is a process of analyzing and estimating possible future events, considering various alternatives
Sensitivity analysis	Sensitivity analysis helps in determining which risks have the most potential impact on the project by figuring how “sensitive” a model is to varied input parameters of the model and to changes in its structure
Fuzzy logic	It is characterized by adapting to the real world, i.e. it quantifies the belongingness for values by linguistic concepts
Break even analysis	Break-even analysis is a useful tool to study the relationship between fixed costs, variable costs and returns
Analytic Hierarchy Process (AHP)	This is a method for organizing and analyzing complex decisions and is based on mathematical and psychological sciences. Thus, involves the experience, the knowledge and the intuition of the decision makers

Source: Thaheem *et al*. (2012)

Degen *et al*. (2007) showed that lay people and experts in risk mitigation do not use the same approaches of ‘risk mitigation’ when treating risks. Arguably, most quantitative experts (quants) focused on quantitative assessments of likelihood and consequences, whereas the general public and most qualitative analyst use a number of qualitative dimensions such as ‘experience,’ or ‘lack of knowledge to those exposed’ and ‘catastrophic potential’ subjectively (Bayaga and Mtose, 2010). The qualitative analysis has been very influential and has become well known in risk mitigation at the expense of quantitative. Bayaga and Mtose (2010) concluded that the bottom line here is that quantitative and qualitative data are, at some level, virtually inseparable. Neither exists in a vacuum nor can be considered totally devoid of the other. To ask which is better or more valid ignores the intimate connection between them. To do good risk mitigation therefore, analyst need both. One of the most intricate parts accompanying risk mitigation is the quantification of risk (Rebiasz, 2007). Some of these quantitative techniques are less applicable as they necessitate the need for detailed information which is generally not available at the planning stage and thus there is a difficulty in making accurate decisions (Dey, 2010).

Both qualitative and quantitative techniques to risk mitigation have their advantages and disadvantages. Certain situations may call for organizations to adopt the quantitative approach. Alternatively, organizations of small size or with limited resources will probably find the qualitative approach much more to their liking. The comprehensive literature review was carried out for 16 quantitative risk mitigation techniques. They are described in the Table 3.

Risk mitigation in IT governance: The risk mitigation decisions needs to be performed in order to have a proficient decision process in the mitigation of identified risks in IT governance. Poorly defined risk mitigation process in IT governance cause IT projects to fall behind schedule, go over budget and result in poor quality. Decisions will be performed in order to have an efficient solution of risk, thus mitigation of risk aids the management in making decision in IT governance process (Eugene and Loggerenberg, 2006; Khatavakhotan *et al*., 2012). According to Shahzad *et al*. (2011) risk mitigation provides a mechanism for managers to handle risk effectively by providing the step wise execution of risk handling by presenting easy to understand flowcharts to express the working of each mitigation strategy against any risk factors in IT Governance (Table 4).

Faisal *et al*. (2007) stated that the mitigation of risks aids managers to understand the mutual relationships among the enablers of risks mitigation and provides a suitable metric to quantify these risks. Thus, managers are provided with an opportunity to understand the important areas that needs attention to minimize the risks to the real time and free flow of information. Therefore, it gives an opportunity to the management to quantify risks in lean or agile environments and develop suitable strategies to manage them. Khatavakhotan *et al*. (2012) contributed that risk mitigation facilitates the development of comprehensive IT governance plan by focusing on the unseen risks and opportunities accompanying with the risk mitigation decisions. Thus, risk mitigation is important in order to make an effective decision, regarding the identified risks.

Table 4: Qualitative techniques for risk mitigation

Categories	Description
Brainstorming	Brainstorming involves stimulating and encouraging free-flowing conversation amongst a group of knowledgeable people
Delphi technique	The Delphi technique is a procedure to obtain a reliable consensus of opinion from a group of experts
Check-lists	Check-lists are lists of hazards, risks or control failures that have been developed usually from experience
Preliminary Hazard Analysis (PHA)	PHA is a simple, inductive method of analysis whose objective is to identify the hazards and hazardous situations and events that can cause harm for a given activity, facility or system
HAZOP	HAZOP is a structured and systematic examination of a planned or existing product, process, procedure or system
Structured “What-if” Technique (SWIFT)	It is a systematic, team based study, utilizing a set of ‘prompt’ words or phrases that is used by the facilitator within a workshop to stimulate participants to identify risks
Scenario analysis	Scenario analysis is a descriptive models of how the future might turn out
Business Impact Analysis (BIA)	Business impact analysis is analyses how key disruption risks could affect an organization’s operations and identifies and quantifies the capabilities that would be needed to manage it
Root cause analysis (RCA)	RCA is focused on asset losses due to various types of failures. It attempts to identify the root or original causes instead of dealing only with the immediately obvious symptoms
Cause-and-effect analysis	Cause-and-effect analysis is a structured method to identify possible causes of an undesirable event or problem. It organizes the possible contributory factors into broad categories so that all possible hypotheses can be considered
Consequence/probability matrix	The consequence/probability aims to produce a level of risk or risk rating. The format of the matrix and the definitions applied to it depend on the context in which it is used and it is important that an appropriate design is used for the circumstances

Sinha *et al*. (2004) affirmed that risk mitigation provides a disciplinary environment for proactive decision making to assess continuously what could go wrong as well, determine which risks are important to deal with and implement strategies to deal with those risks. He maintained that risk mitigation provides a structural method to conduct risk investigation and make sure that there is less redundancy in IT governance. Besides, Xiao *et al*. (2013) pointed out that risk mitigation emphasizes on taking action early in IT project to prevent the occurrence of undesired events or to reduce the consequences of their occurrence. These mitigation actions helps project managers to appropriately planned and such plans mitigation plans include estimating and planning the schedule, resources and funding for mitigation in optimization of project cost and schedule.

Khatavakhotan *et al*. (2012) report that risk mitigation stabilizing the requirements, designs and implementations in software development, also an integrated risk mitigation plan aids the risk manager in carrying out his core responsibility as well as a main concern in IT governance. Furthermore, Tran and Liu (2007) mentioned that risk mitigation is important because it focuses on identifying strategic and tactical approaches to minimize the negative impacts of the identified risks to the systems overall functionality, reliability, performance and maintainability and lastly, Xu *et al.* (2005) added that risk mitigation is important to IT Governance because it provides managers with an effective tool to make the risk control decisions and implement the process optimization at the project planning stage.

Risk mitigation models and frameworks: The reviewing of risk mitigation is the most discussed issue in literature specifically relating to the previous model or framework. There are many risk mitigation models which have been developed in previous research works, all of the 14 models that have been reviewed have their own strengths and weaknesses since the researchers try to improve upon one another’s design, or focus on different contexts. Furthermore, these models give clear definitions related to the concept of risk mitigation and risk factors based on the context of the studies. However, most of them are lacking in clear explanation related to risk mitigation in detail. The review study related to risk mitigation models are depicted in Table 5.

Currently, there are numerous risk mitigation models available. Some of which are qualitative while others is quantitative in nature. These models have a common goal of mitigating the overall risk value. However, there are no methods which will assist organisations in determining which model is the best to be employed within an organization.

There are numerous risk mitigation models nowadays and many more emerging every day. They all have the same basic goal, even though try to achieve it through very different perspectives and addressing problems differently. Some of them can be applied to all kinds of risk, other are specific for particular risks. The main purpose of the report is to compare and clarify the different activities, inputs and outputs required by each risk mitigation models, their issues and then analyze which ones address risk effectively. The resulting information helps evaluating the models’ applicability to an organization and their specific needs.

This study presents a systematic literature review that investigates risk mitigation of IT governance. The aim is to identify and characterize different frameworks that are used to assess risk in IT governance to provide a comprehensive outline and discussion of methods, standards and techniques used in risk mitigation in IT governance, however, one of our findings suggests that more papers were published in 2005 in relation to our research risk mitigation and IT Governance.

Also we can see that risk mitigation is a part of IT governance, since it’s a sub of process that need to be concern in IT governance activities and implementation. From our SLR we found out that risk mitigation is one of the main activities in risk management of IT governance. Based on our review, we finds that the Information Technology Infrastructure Library (ITIL) is considered one of the appropriate best practice model for ICT governance and service management

Table 5: Risk Mitigation models of information technology

Model and researcher	Components/Technique	Problem solved
A novel model for software risk mitigation plan Khatavakhotan *et al*. (2012)	Proposed a model that involves creating risk mitigation plan, defining triggers, designing a contingency plan and driving the actual risks	Reduce the risks consequences and their occurrence probabilities
	Use benchmark method using quantitative formula as a technique	Identifying effective factors in fault tolerance, the risks consequences and presenting solutions to reduce the risks
Trival model for risk mitigation in software development life cycle (Shahzad *et al*., 2011)	Risk identification, risk factor, avoidance, management. Use avoidance strategy as a technique	Not only focuses on the identification of the risks but also provides a mechanism to handle them effectively Presents the easy to understand, flowcharts to express the working of each mitigation/avoidance strategy against any risk factors
A generic prescriptive methodology for mitigating risks (Sinha *et al*., 2004)	Components includes, identify risk, assess risks, plan solution, conduct failure modes and effect analysis and continuous improve. Use hypothetical case study as a technique	Presented a structured methods to conduct risk investigation and make sure that there is less redundancy in the mitigation process
Model based mitigation of available risks (Zambon *et al*., 2007)	Divided into 2 basic components of risk evaluation and risk mitigation. Qualitative based technique	Works with other models to carry out a risk mitigation activity which allows to assess the global impact of a set of risks and to choose the best set of countermeasures to cope with
A risk mitigating model for integrated software systems (Tran and Liu, 2007)	The inputs to the model consist of identification, evaluation and integration/enhancement	Effectively identify and address these potential technical risks, using a risk mitigating and systematic approach to software product evaluation and integration
A conceptual framework to quantify and mitigate information risk (Faisal *et al*., 2007)	The theoretical model involves identify information risk variable, develop information risk variable digraph, transform digraph into matrix form, using suitable scale, evaluate permanent function and information risk index Technique use is quantification, graph theory and interpretive structural modelling	Focus on IS particularly on the mitigation aspect of various information risks that could impact the flow of information in a supply chain network. Provides the managers with an opportunity to understand the focal areas that needs attention to minimize the risks to the real time and free flow of information. Enables decision makers to quantify the impact of various variables of information risks in the final outcome
Qualitative method-based the effective risk mitigation (Eom *et al*., 2006)	The model consists of key variables such as the results of risk analysis, safeguard methods, safeguard techniques, risk acceptance, cost benefit analysis, safeguard decision and safeguard implementation. Qualitative safeguard technique was used	The model helps in risk reduction safeguard's method/ technique according to risk type, and performed cost-benefit analysis
Risk mitigation framework for a robust design process (Narania *et al*., 2008)	Risk identification, Risk assessment and Risk mitigation. Technique is quantification and prioritization used to evaluate and rank risks	Help identify, assess and mitigate the risks associated with the development and insertion of technologies in a Manufacturing environment
A risk mitigation model in SME (Coras and Tantau, 2013)	Power empowerment, communication, trust, learning, leadership and ethic-behaviour qualitative approach was used as a technique	The research results indicate six factors as main risk mitigates by managing and mitigating the effective risks triggered by open innovation in SMEs
A framework for risk identification and mitigation processes for using scrum in global software development (Hossain *et al*., 2009)	Asynchronous, lack of group awareness, poor communication, lack of tool support, large number of project personnel, lack of collaborative office environment and increased number of sites. Using Scrum as technique	Expected to help Global Software development practitioners to understand the risk factors they may need to consider while using Scrum
Mitigation of software risk management process model (Khatavakhotan *et al*., 2012)	Components of risk reduction, circumferential risk, arisen opportunities and amplified opportunities. Use a synthesized approach	The model facilitates the development of comprehensive risk mitigation plan by focusing on the unseen risks and opportunities accompanying with the risk mitigation decisions, which are basically ignored in the other models
Search based risk mitigation planning model (Xiao *et al*., 2013)	Proposed a model that takes the from of risk identification and analysis, risk and candidate mitigating actions, projects and activities and plan and risk mitigation. Used a search based software engineering (SBSE) approach	Problem of mitigating risk in software projects and the model can identify effective risk mitigation plans, thus providing useful decision support for managers
An innovative model for optimizing software risk mitigation plan (Khatavakhotan and Ow, 2012)	The components includes risk identification, risk measurement, risk assessment, risk mitigation decision and integrated risk mitigation plan. The researchers uses the historical data technique and synthesis formula	The model considers the circumferential risks and opportunities in mitigation process. This fact has been ignored in the current models. However this model adds some costs to the risk process, but its remarkable benefits will compensate the expenses. The model leads to an integrated mitigation plan for unseen risk
A model for evaluating and mitigating information systems project risk (Liu *et al*., 2009)	The inputs to the model consist of three sets risk index, risk evaluation and risk mitigation Based on balanced score card (BSC) technique	Integrating strategy and risk mitigation effectively in which strategies are distributed, BSC can be a tool for reducing the IS development risks and improving development performance while guarantee the realization of target

and it is also recommended to supplement the COBIT and the ISO 17999 for dealing with ICT risk management (ITGI., 2008). Further research work will be study on risk mitigation of the IT governance that able to assist in develop tool for assessing the IT governance risk in IT project.

CONCLUSION

In conclusion, the obtained findings, including an examination of the shortcomings found in this systematic literature review, provide strong evidence to encourage further research in the development of a new methodology to adequately perform risk mitigation in IT governance. Mitigating risk is a key factor and a major requirement to secure successful IT projects including IT governance. Findings obtained that in current environment, there are risk mitigation models available, some of which uses qualitative technique while others are quantitative in nature. These models have a common goal of mitigating the overall risk but in order to address the risk challenge in current and future situation of IT projects and its governance, a risk mitigation models is suggested to incorporate both knowledge codification and agent technology in their consideration. This research will introduces a risk mitigation model that is being developed for mitigating the risks associated with in IT Governance even not much historical information and previous literatures are available as well as help to predict the risk. Also, the proposed model will deal with the risks of variation, from the designed nominal values which are always inherent in any, IT governance process and faster decision making process.

REFERENCES

Aloini, D., R. Dulmin and V. Mininno, 2012. Risk assessment in ERP projects. Inform. Syst., 37: 183-199.

Bayaga, A. and X. Mtose, 2010. Quantitative risk analysis: Determining university risk mitigation and control mechanisms. J. Int. Soc. Res., 3: 55-68.

Bodnar, G.H., 2003. IT governance. Internal Audit., 18: 27-32.

Brereton, P., B.A. Kitchenham, D. Budgen, M. Turner and M. Khalil, 2007. Lessons from applying the systematic literature review process within the software engineering domain. J. Syst. Software, 80: 571-583.

Coras, E.L. and A.D. Tantau, 2013. A risk mitigation model in SME's open innovation projects. Manage. Market., 8: 303-328.

Degen, M., P. Embrechts and D.D. Lambrigger, 2007. The quantitative modeling of operational risk: Between G-ANDH and EVT. Astin Bull., 37: 265-270.

Dey, P.K., 2010. Managing project risk using combined analytic hierarchy process and risk map. Applied Soft Comput., 10: 990-1000.

Eom, J.H., S.H. Lee, H.J. Lim and T.M. Chung, 2006. Qualitative Method-Based the Effective Risk Mitigation Method in the Risk Management. In: Computational Science and Its Applications, Gavrilova, M.L., O. Gervasi, V. Kumar, C.J.K. Tan and D. Taniar *et al*. (Eds.). Springer, Berlin, Germany, ISBN: 978-3-540-34072-0, pp: 239-248.

Eugene, W. and J.V. Loggerenberg, 2006. IT governance: Theory and practice. Proceedings of the Conference on Information Technology in Tertiary Education, September 18-20, 2006, Pretoria, South Africa, pp: 1-14.

Faisal, M.N., D.K. Banwet and R. Shankar, 2007. Information risks management in supply chains: An assessment and mitigation framework. J. Enterprise Inform. Manage., 20: 1747-17398.

Hossain, E., M.A. Babar, H.Y. Paik and J. Verner, 2009. Risk identification and mitigation processes for using scrum in global software development: A conceptual framework. Proceedings of the 16th Asia-Pacific Software Engineering Conference, December 1-3, 2009, Penang, Malaysia, pp: 457-464.

ITGI, 2001. Board Briefing on IT Governance. IT Governance Institute, UK.

ITGI., 2005. COBIT. 3rd Edn., IT Governance Institute, UK, pp: 1-10.

ITGI., 2008. Board Briefing on IT Governance. IT Governance Institute, UK pp: 1-20..

Karabacak, B. and I. Sogukpinar, 2006. A quantitative method for ISO 17799 gap analysis. Comput. Security, 25: 413-419.

Khatavakhotan, A.S. and S.H. Ow, 2012. An innovative model for optimizing software risk mitigation plan: A case study. Proceedings of the 6th Asia Modelling Symposium, May 29-31, 2012, Bali, Indonesia, pp: 220-224.

Khatavakhotan, A., N. Hashemitaba and S.H. Ow, 2012. A novel model for software risk mitigation plan to improve the fault tolerance process. Int. J. Inform. Technol. Comput. Sci., 5: 38-42.

Kitchenham, B. and S. Charters, 2007. Guidelines for performing systematic literature reviews in software engineering. Joint Technical Report Software Engineering Group, Dept. of Computer Science, Keele University, UK and Empirical Software Engineering, National ICT, Australia, pp: 45-56.

Kumsuprom, S., B. Corbitt and S. Pittayachawan, 2008. ICT risk management in organizations: Case studies in Thai business. Proceedings of the 19th Australasian Conference on Information System, December 3-5, 2008, Christchurch, New Zealand, pp: 513-522.

Lainhart, J.W., 2000. Why IT governance is a top management issue. J. Corp. Account. Finance, 11: 33-40.

Lientz, B.P. and L. Larssen, 2006. Risk Management for IT Projects: How to Deal with Over 150 Issues and Risks. Routledge, UK., ISBN: 9780750682312, Pages: 331.

Lin, Y.M., N.H. Arshad, H. Haron, Y.B. Wah, M. Yusoff and A. Mohamed, 2011. IT governance awareness and practices: An insight from Malaysian senior management perspective. J. Bus. Syst. Governance Ethics, 5: 43-57.

Liu, S., T. Chen, Y. Liu and J. Zhang, 2009. Evaluating and mitigating information systems development risk through balanced score card. Proceedings of the International Symposium on Information Engineering and Electronic Commerce, May 16-17, 2009, Ternopil, Ukraine, pp: 111-115.

Mellado, D. and D.G. Rosado, 2007. An overview of current information systems security challenges and innovations. J. Universal Comput. Sci., 18: 1598-1607.

Narania, S., T. Eshahawi, N. Gindy, Y.K. Tang, S. Stoyanov, S. Ridout and C. Bailey, 2008. Risk mitigation framework for a robust design process. Proceedings of the 2nd Electronics System-Integration Technology Conference, September 1-4, 2008, Greenwich, UK., pp: 1075-1080.

Rebiasz, B., 2007. Fuzziness and randomness in investment project risk appraisal. Comput. Operat. Res., 34: 199-210.

Saint-Germain, R., 2005. Information security management best practice based on ISO/IEC 17799. Inform. Manage. J., 39: 60-66.

Shahzad, B., Y. Al-Ohali and A. Abdullah, 2011. Trivial model for mitigation of risks in software development life cycle. Int. J. Phys. Sci., 6: 2072-2082.

Sinha, P.R., L.E. Whitman and D. Malzahn, 2004. Methodology to mitigate supplier risk in an aerospace supply chain. Supply Chain Manage.: Int. J., 9: 154-168.

Sommerville, I., 2011. Software Engineering. 9th Edn., Pearson Inc., USA., ISBN: 9780137053469, Pages: 773.

Thaheem, M.J., A. De Marco and K. Barlish, 2012. A review of quantitative analysis techniques for construction project risk management. Proceedings of the Creative Construct Conference, June 30-July 3, 2012, Budapest, Hungary, pp: 656-667.

Tran, V. and D.B. Liu, 2007. A risk-mitigating model for the development of reliable and maintainable large-scale commercial-off-the-shelf integrated software systems. Proceedings of the Annual Reliability and Maintainability Symposium, January 13-16, 2007, Philadelphia, PA., pp: 361-367.

Von Solms, B., 2005. Information security governance: COBIT or ISO 17799 or both? Comput. Security, 24: 99-104.

Xiao, J., L.J. Osterweil, J. Chen, Q. Wang and M. Li, 2013. Search based risk mitigation planning in project portfolio management. Proceedings of the 2013 International Conference on Software and System Process, May 18-19, 2013, San Francisco, CA, USA., pp: 146-155.

Xu, R., P.Y. Nie, Y. Sai, L.H. Qu and L. Yun-Ting, 2005. Optimizing software process based on risk assessment and control. Proceedings of the 5th International Conference on Computer and Information Technology, September 21-23, 2005, Shanghai, China, pp: 896-900.

Zambon, E., D. Bolzoni, S. Etalle and M. Salvato, 2007. Model-based mitigation of availability risks. Proceedings of the 2nd IEEE/IFIP International Workshop on Business-Driven IT Management, May 21, 2007, Munich, Germany, pp: 75-83.