JOURNAL OF SOFTWARE ENGINEERING & INTELLIGENT SYSTEMS
ISSN 2518-8739
31st December 2016, Volume 1, Issue 2, JSEIS, CADMEI Copyright © 2016
www.jseis.org

Knowledge mapping and multi-software agents based system for risk mitigation in IT organizations

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

ABSTRACT

As the reliance on information technology (IT) in running organizations services is increasing, so is the exposure to the associated risks due to IT use. In IT organization rules, policies and procedures are put in place by management in organizations to ensure the IT Infrastructures (Hardware, Software and Network Communication devices) are used effectively to achieve the objectives of the organization. In order to achieve the objectives, set by management, risks need to be mitigated effectively and adequately. Risk mitigation involves the risk identification, risk decision, risk treatment and risk monitoring and risk report. However, available risk mitigation tools/systems present many weaknesses and above all, they are limited. The objective of this paper is to present a risk mitigation system (RMS) tool for risk decision in mitigating risk that occurs in IT organization. The RMS is developed based on the risk decision process, for mitigating risk, that has been developed in this research. The tool is developed using multi-software agents and knowledge mapping. Findings from this paper shows how the tool can support mitigation of risk thus providing decision support for IT managers, and IT practitioners in their organization.

Keywords: Risk; risk decisions; risk mitigation; software agents; knowledge mapping

1. INTRODUCTION

Risk is considered as something that might go wrong in an establishing process. Risk is also a combination of the likelihood of an event and its effects. In IT organization management s must learn to stabilize the possible negative effects of risk against the possible gains of its related opportunity [1]. Risk mitigation emphasizes taking action early in IT organization to prevent the occurrence of undesired events or to reduce the consequences of their occurrence. These mitigation actions should be appropriately planned, and such plans should include estimating and planning the schedule, resources, and funding for mitigation. Once a risk is identified, mitigation actions should be identified. But since most risks can be mitigated in quite a few different ways, each of which may require different resources at different times. Therefore, selecting the best mitigation action is not an easy task for practitioners [2]. Risk mitigation involves risk identification, risk decision, risk treatment and risk monitoring. Risk mitigation is an essential component of IT organization and plays a significant role in IT organization success. IT organization supports business operations, adding value through IT component and risks mitigation. The purpose of IT organization is to direct IT endeavors to ensure that IT performance meets the objectives set out in its strategy. With effective IT organization, the return of IT investment can be optimized to support business strategies and goal [1]. Risks can be mitigated with the correct organizational decision-making structures and the assignment of roles and responsibilities. Decision making is a process by which a person, group, or organization identifies a choice or judgment to be made, gathers and evaluates information about alternatives. This definition implies that decision-making involves risks in selecting one from several courses of action, which is usually compounded by time and information constraints. In IT organization, decision making relating to risk mitigation is perceived by the top management as a technical problem [3]. To mitigate risk, management must have effective means for mitigating operational, technical and strategic risks. IT organizations faces operational, technical and strategic risks that prevent practitioners in attaining their planned schedule, time and quality in when using IT Infrastructures (Hardware, Software and Network Communication devices).

As a result, risk mitigation procedures put in place in organizations tend to be inadequate. Furthermore, the traditional way of mitigating risks by transferring them to insurance companies is not working effectively, as it is difficult to estimate the consequences due to IT-related risks. Existing available tools for risk mitigation are mainly designed for risk analysis and evaluation [4]. Several risk tools lacked capabilities to support IT managers in IT organization environment to mitigate risks that occurs with usage of IT infrastructures. Currently there are only risk mitigation standards and guidelines and inadequate risk mitigation tools to provide support for mitigation operational,

technical and strategic risk that occur in IT organization. The existing tools are lacking in capturing and reuse of lessons learnt from previous events, case studies and best practices, to utilize and disseminate the previous as well as existing knowledge and experience within the practitioners and decision makers in IT organization. These tools also lack in assisting IT managers, practitioners and decision makers in identifying the cause of risks experienced when utilizing IT infrastructures [5].

Therefore, there is a need for a tool which can assist in solving operational, technical and strategic risks and thereby creating a common understanding of these risks among technical people and the management within IT organization. With a common understanding, it would be possible to realize a coordinated approach towards risk mitigation in IT organization [6]. Risk mitigation tool is also needed to assist practitioners in making decision in risk mitigation. The implemented Risk Mitigation System (RMS) automatically identifies the operational and technical risk data directly from knowledge base, establishes risk description according to risk measurement schemes, generates and display risk report for decision making. RMS uses an agent-based system that supports risk mitigation as an iterative and continuous process across large-scale collaborative teams in IT organization. RMS assist in identification of risk, making decision on risk, provide solution on risk treatment and assist IT practitioners in monitoring identified risks.

RMS also measures the identified risk using agents to quantify the risk probability and risk impact. The measuring agent in RMS measure the risk by assigning different color to the risk probability and impact based on the risk severity and impact to IT organization. The RMS tool aids the knowledge retrieving, storing, sharing process by mapping knowledge in the knowledgebase. The rest of this paper is organized as follows. Section 2 describes literature review. Section 3 describes the methodology. Section 4 describes the risk mitigation practice. Section 5 shows the RMS implementation. Section 6 presents the discussion and conclusions section.

2. LITERATURE REVIEW

This section briefly explores on the concepts of risk, importance of risk mitigation in IT organization and the need for decision making in mitigating risk in IT organizations.

a) Overview of risk in IT organizations

Risk can be normally an unseen occurrence. Risk is also a combination of the likelihood of an incident and its effects [7]. Risk in itself is not bad; risk is crucial to develop, and failure is normally a key part of knowledge. But management must learn to treat the possible negative effects of risk against the possible gains of its related opportunity [8]. Risk occurs when IT infrastructures are used to accomplish the aims and objectives of IT organization. In IT organization, the lack of open communication, forward-looking attitude, team involvement in the practitioners, management and the knowledge of typical problems, exposes IT infrastructures (hardware, software, network devices and other peripherals) to operational and technical risk.

Risk process in IT organization starts with the identification of existing operational and technical risks. Once the risks are identified, they are evaluated and measured and then appropriate mitigation actions are planned and executed. To reach the acceptable level of success guarantee, the introduced actions must be controlled and the risks in mitigation must be continuously monitored for their status [9].

b) Importance of risk mitigation in IT organizations

In risk mitigation, the practitioner and management perspective is included in the treatment of IT risks by identifying, evaluating, minimizing, and controlling potential IT risks in IT organization process [10]. Risk mitigation is a good practice and can assist with meeting a range of compliance, statutory, organizational and governance requirements. By effectively mitigating the risks IT organization faces, management can guard against poor decision making. According to [11] mitigation of risk provides a mechanism for managers to handle risk effectively by providing the step wise execution of the risk handling methodology, presenting the easy to understand, flowcharts to express the working of each mitigation strategy against any risk factors in IT organization.

In a research study [12], it is 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 focal areas that needs attention to minimize the risks to

the real time and free flow of information. This would help the decision makers to estimate the impacts of various risks and consequently develop suitable strategies to counter them.

The research study [13] contributed that in risk mitigation decisions will be performed in order to have an efficient decision in the mitigation of identified risks, meaning that mitigation of risk aids the management in making decision in IT organization. Risk mitigation facilitates the development of comprehensive IT organization plan by focusing on the unseen risks and opportunities accompanying with the risk mitigation decisions, which are basically ignored in IT organization process, thus risk mitigation is important in order to make an effective decision, regarding the identified risks. The research study [14] affirms that risk mitigation provides a disciplinary environment for proactive decision making to assess continuously what could go wrong, determine which risks are important to deal with and implement strategies to deal with those risks. They maintained that risk mitigation provides a structural method to conduct risk investigation and make sure that there is less redundancy in IT organization.

The research study [15] pointed out that risk mitigation emphasizes on taking action early in a project to prevent the occurrence of undesired events or to reduce the consequences of their occurrence. These mitigation actions help 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. The research study [16] reports that risk mitigation stabilizes 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 organization.

The research study [17] stated 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. Lastly, the research study [18] added that risk mitigation is important to IT organization because it provides managers with an effective tool to make the risk control decisions and implement the process optimization at the project planning stage.

c) Related works

IT practitioners need to ensure delivery of IT requirement when using IT infrastructures. This usually involves mitigating the operational and technical risks that occurs. Research related to risk mitigation has attracted steady stream of interest in the academic literature, in spite of scholars and practitioners recognizing the risk mitigation models in IT projects. Insufficient attention has been paid by researchers to select a suitable risk mitigation model or tool. This section attempts to address this limitation and the gap in the current literature and later provide a model and tool for mitigating risk in subsequent sections.

The research in [19] defines a method consisting of risk evaluation/risk mitigation and a tool for carrying out risk mitigation activity by assessing the global impact of a set of risks and to choose the best set of countermeasures to cope with them. The tool provided a more precise risk mitigation activity. The tool is criticized for not having a knowledgebase to save risk mitigation activities and results. [20] presented a model and prototype developed to identify, estimate, document, assess, prioritize, monitor, control and displays statistics of the risk in a less complex interface, easy-to-use, efficiency and less time consuming risk tool.

The tool can only be used as an application and cannot be assessed on the web. [6] designed a model and EMITL tool consisting of state risk; risk analyze, risk findings and risk counter measures. The tool assist in mitigating IT risks based on risk exposure and setting countermeasures for the risk. The tool only helps in quantifying IT related risk for management and technical department.

The research in [5] developed an intelligent risk mapping and assessment system model and tool (IRMAS) involving risk identification, risk impact and weight analysis, event drivers' identification, risk probability and magnitude analysis, risk mitigation and risk management plan. The tool is designed to identify, prioritize, analyze and assist project managers to mitigate perceived sources of risks. [21] presented a model and tool Analyzer for Reducing Module Operational Risk (AMOR) consisting of risk metrics, risk Modelling, evaluation, risk assessment, risk prediction, display risk result for decision making, however, the complete functionality of ARMOR is not yet implemented. [3] developed a web-based system based on their proposed model.

The model consists of risk identification, analysis, evaluation, response and monitoring, which enabled users almost anywhere to perform continuous risk mitigation for each stage of decision processes. The researchers quantified

the risk in a systematic manner such that the causal relationships between risks can be understood by the decision makers. [4] developed a model and an agent based risk tool. The model process involves context establishment, risk identification, risk impact and probability analysis and risk mitigation. The researchers developed a web-based system that supports risk mitigation as an iterative and continuous process across collaborative teams. [22] propose RIAP (Risk Identification Architecture Pattern) model to manage risks in Web projects. It has been implemented in a tool called WPRiMA (Web Project Risk Management Assessment). WPRiMA support IT process to estimate and mitigate risk. [23] proposed a web-based application that is implemented based on the functional risk classification and assessment model. The tool is useful for making decisions to mitigate IT risks by incorporating a different scale, estimating risk probabilities from historical data and providing more flexibility to the Decision Making. [24] proposed a risk assessment model and hospital information system (HIS) tool for mitigating risk when there is no sufficient data. The tool integrates possible risk factors into the decision-making process of risk assessment. In the model, a reality-design gap analysis is used to determine risk likelihood instead of directly risk evaluation and integrates to the decision-making process for risk mitigation. [9] develop a collaboration model that helps to identify, analysis, plan, track, control and communication risk mitigation. Showing the roles and communication paths among the teams to support risk mitigation activities as well as supporting the collaboration among risk teams. The researchers then present a tool called Risk-Guide that supports the risk mitigation using checklists together with qualitative risk evaluation.

d) Knowledge mapping and multi-software agents

This section explores on knowledge mapping and agent technology. Knowledge is information in action in which data are extracted and transformed into information, and load them into databases. Having acquired information from data and storing it in a data warehouse, information need to be transformed into knowledge [25]. As practitioners try to mitigate risk in IT organization, there is need for an innovation to produce the knowledge intensive services desired by decision makers.

Knowledge mapping in risk mitigation context is in its infancy and has the potential to address both operational and technical risk faced in IT organization. Knowledge map is a picture of what exists in an organization or a network. Therefore, it can be used as a tool to mitigate risk in IT organization. Knowledge mapping is the field within knowledge management that aims to optimize the efficient and effective use of the organization's knowledge. Developing a knowledge map involves locating important knowledge within the organization and then publishing some sort of list or picture that shows where to find it [26]. Knowledge maps typically point to people as well as to documents and databases [27]. Knowledge mapping is one way that allows knowledge to be represented graphically through nodes to represent main ideas and links leading to representing the relationships between the ideas. Knowledge map is the best tool to represent knowledge in an organization [28] The elements which are mapped onto such a shared context range from experts, practitioners, or communities of practice to more explicit and codified forms of knowledge, such as white papers or articles, patents, lessons learned, or databases [26].

In information technology, an agent is software that acts or brings about a certain result; it is one who is empowered to act for another [29]. Agent can be defined as a software entity, which is autonomous to accomplish its design objectives, considered as a part of an overall objective, through the axiom of communication and coordination with other agents [30]. According to [31] in software system, agent means software component that can interact autonomously as a substitute for its user with its environment and other agents to achieve the predefined goal [31]. [30] stated that agent based technology is acknowledged as one of the most promising technologies for effective mitigation of risk. Moreover, agents can be integrated in risk mitigation model in IT organization to forecast risky situations. Agents can work together to create models that can change over the time and adapt to the changing conditions of the environment, thus, making possible to detect risky circumstances in IT organization and providing recommendations and approvals that can help to mitigate possible unwanted risk [32].

Through agent learning capability, they can demonstrate efficiently the proactive and autonomous behavior of participating agents in mitigating risks in real time [32, 33]. [30] added that the interactions among these agents were subsequently developed by analyzing several risk identification and mitigation processes. [30] stated that the use of multi-agent Modelling can be an alternative decision making tool for risk mitigation and collaboration. Thus Knowledge Mapping and software agent are to be used as techniques in the model to assist in risk mitigation decision making in IT organization. Agents assist managers and other decision makers to identify, sufficiently early, the risks associated with IT organization, development, integration, and deployment so that appropriate mitigation strategies

can be implemented on a timely basis [29]. Software agents create and store explicit knowledge as declarative memory through mapping a process by which explicit knowledge is created from information and stored in repositories for repetitive and routine querying [25].

3. METHODOLOGY

This section discusses the methodology that has been considered in implementing the RMS tool. Four phases were covered in developing the tool. The 4 different phases are as follows:

- Phase – 1: Literature Review
- Phase – 2: RMS Pseudocodes and Agents Algorithms
- Phase – 3: Adopt a System Development Life Cycle
- Phase – 4: Code the RMS Tool

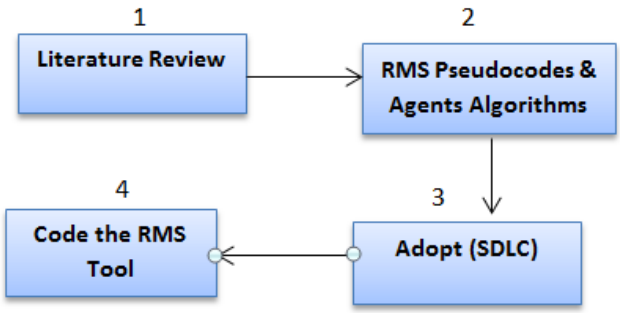

Figure. 1 Methodology for RMS Implementation

Figure 1 shows the phases followed to implement the risk mitigation system.

3.1 Methodological process

The phases and activities carried out to implement the RMS tool are shown below;

a. Phase 1: Literature Review
Phase 1 encompasses the reviewing of journals, articles and books on exiting risk tools aimed at mitigating risk in IT process. This phase helps in identifying the strength and weakness of exiting tools.

b. Phase 2: RMS Pseudocode and Agent Algorithms
This phase involves the development of risk pseudocode and agents algorithms. The various agents that assist in making the risk decisions in mitigating risk are shown in this phase.

c. Phase 3: Adopt SDLC
d. Phase 4 involves the adoption of the system development life cycle in the implementation and coding of the risk mitigation system.
e. Phase 4: Code the RMS Tool
f. Phase 5 involves the programming of the system using PHP for the agents and functions, MYSQL for the risk knowledge base via knowledge mapping technique, JavaScript for the system and CSS for a responsible and useable system.

3.2 Risk decision process

This section explores on the risk decision process. The risk decision process helps to make decision in mitigating risk in IT organizations. The risk decision process is seen in Figure 2.

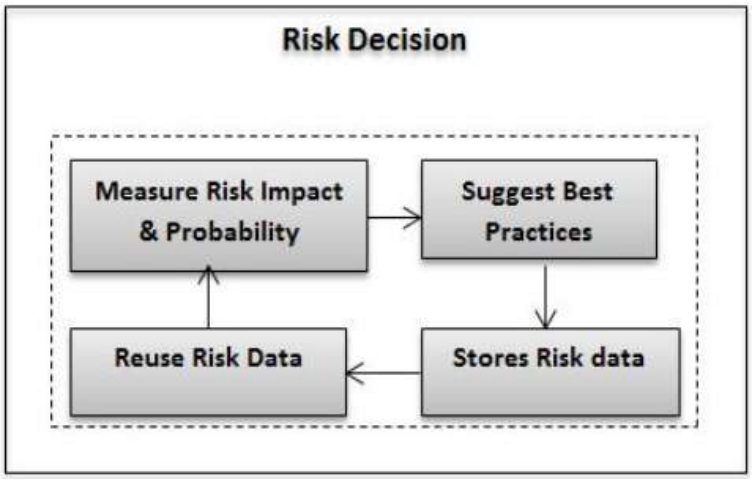

Figure. 2 Risk decision process

Figure 2 shows the risk decision process. The process assists in providing support to practitioners in making decisions on risk mitigation.

3.3 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 the 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 as seen in Figure 3, Table 1 and Table 2 in this paper. 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 [34].

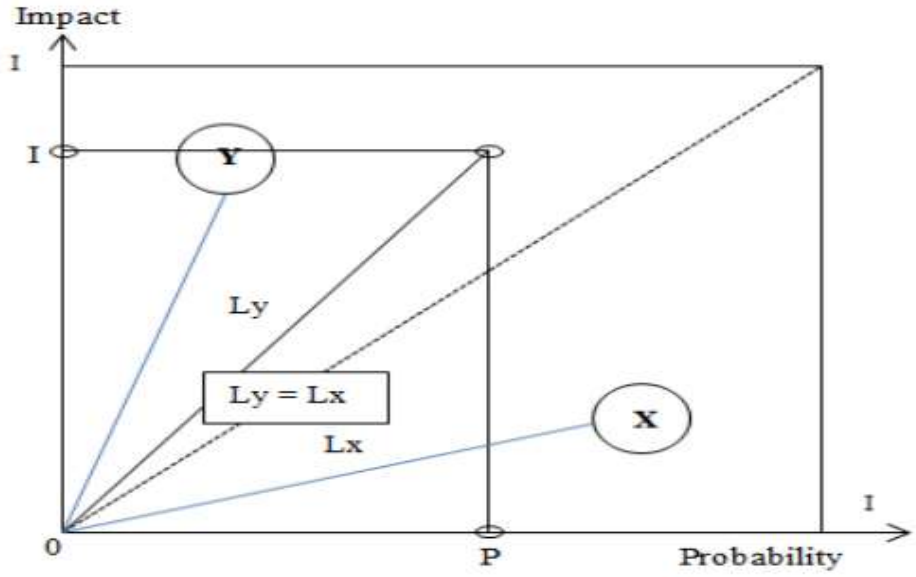

Figure. 3 Consequences and probability matrix [35]

Figure 3 shows the consequence and probability matrix is used by the measurement agents to measure the identified risk magnitude based on the risk impact and risk probability.

Table. 1 Probability scoring guideline for risk mitigation

Value	Probability Level
9-10	Very likely to occur
8-7	Will probably to occur
6-5	Equal chance of occurring or not
4-3	Probably not occur
1-2	Very unlikely

Table. 2 Impact scoring guideline for risk mitigation

Value	Impact Level
9-10	Very Significant
8-7	Significant
6-5	Significant and insignificant is equal
4-3	Insignificant
1-2	Very insignificant

Table 1 and Table 2 shows the probability and impact scoring guideline for mitigating risk based on the measurement of the risk to be mitigated. The measurement is used by the agents to measure the risk. The application of this can be seen in Figure 6 and Figure 7 in this research paper.

3.4 Best practice suggestion

Best practices are based on previous risk mitigation cases acquired 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.

3.5 Risk data storage

The knowledge base is collation of 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 organization. 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 identify location of critical risk items which are identified based on success factors from lessons learnt.

3.6 Reuse 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 identified operational and technical risk 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. RISK MITIGATION SYSTEM IMPLEMENTATION

This section explores in detail on how the risk mitigation system (RMS) is developed and implemented;

4.1 System development life cycle methodology

This phase involves the development methodology used for the development of the risk mitigation system (RMS). System development life cycle (SDLC) methodology defines a proper detailed process to specify, implement and test/debug agent-oriented software systems. SDLC methodology offers a set of detailed guidelines that includes examples and heuristics, which help better understanding what is required in each step of the development. (SDLC) is used to develop the prototype system. SDLC comprises of five phases; requirement analysis, system design, implementation, testing and evolution as seen in Figure 4.

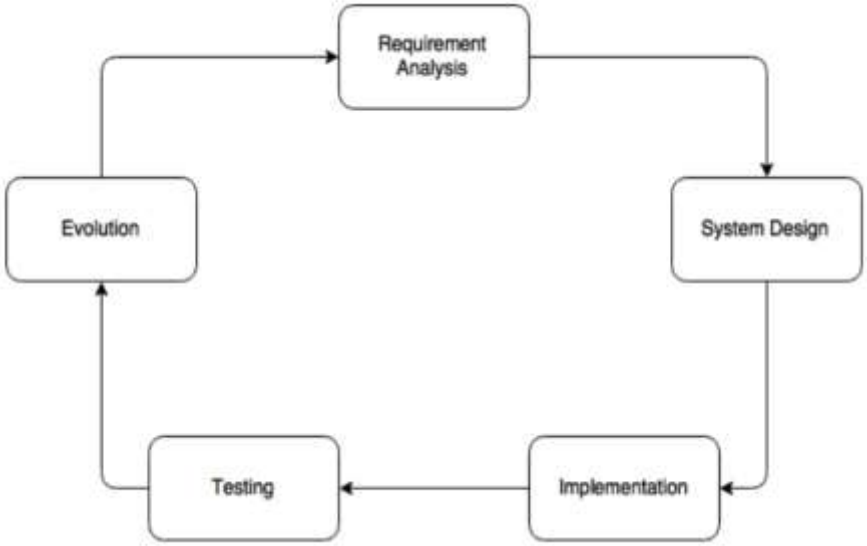

Figure. 4 SDLC methodology

This phase shown in Figure 4 aids to develop a risk mitigation system based on the risk decision process shown in Figure 2 to provide support to practitioners in making decisions based on a risk knowledge base.

a. Requirement analysis

This phase determines who is going to use the system. In this research the users of the system are the Experts, Manager and staffs. This phase also determines how users will use the system either via a web-based system or application based platform. Requirement analysis defines what data should be inputted into the system, the operational and technical data, risk documents and files. Requirement analysis also defines what data should be output by the system, which includes the risk report and risk documents/files to be used by decision makers for risk mitigation in IT organizations.

b. System design

This phase determines the system architecture to be used in deploying the risk mitigation system. 3-Tier Client/Server Architecture, Multi-platform application was used to run the system. This phase also determines the system interface design. Thus, the system interface is simple and easy to use in making decision in mitigating risk as seen in Figure 6 and Figure 7 in this paper.

c. Implementation

This phase involves the coding of the risk mitigation system (RMS) using HTML5, CSS, PHP, MySQL, and JavaScript to support practitioners in mitigating operational and technical risk in IT organizations.

d. Testing

This phase involves running the developed risk mitigation system (RMS) in XAMPP software to test the implemented system against the requirements and detect any errors and bugs in the implemented RMS tool.

e. Evaluation

This phase involves the future functions that can be integrated into the system to see what improvement can be made. It involves the evolution of the RMS in response to changing practitioner needs.

4.2 Risk mitigation system pseudocode

The RMS tool uses software agents to collect practitioners' inputs, risk history and procedures which can assist to mitigate each risk separately for those mentioned in the operational and technical risk table. Risk table is a list of risks encountered by the agent in previous projects. When the particular risk is run for the first time, it will not have any entries in the risk table. The table is formulated by learning the environment. The agent observes the changing trends in IT organizations and suggests suitable modifications in the procedures. From this experience, the learning element can formulate a rule as to which risk mitigating method can be retained, which can be removed, which is outdated etc. [33]. Each of the different risks has different risk mitigation advice and monitoring process. The multi-software agents are also possessing learning ability as seen in the pseudocode below;

```
function risk-based-learning-agent (percept)
returns an action
static: percepts, a sequence, initially empty
history: generic operational & technical risks,
a sequence of possible risks in any project
append generic operational & technical risks
percepts to the end of percepts to the
end of percepts
action  <<<------ Add to the risk table
return action
end
}
```

The pseudocode above shows the initial execution of the operational and technical risk agent; the agent does not have any knowledge of what kind of risks IT infrastructure will be encountered with. As the system learns from its environment, the risk agents' gives feedback on the situation of the risk mitigation process. The knowledge collected agent receives risk inputs from the learning element and the measurement agent formulates the risk measurement. This decides the entire list of risks generated. Risk report is hence automated without the intervention of the experts. The entire system of goal-based learning agent works on the fact that the agents constantly learns from the history as well as the environment. A partial pseudo code for the component of the agent learning risk from the environment can be given as follows:

```
procedure retrieve_GR (input: X, vp , sf; output: K)
{
begin
increment 0;
repeat
for each case i ?
X do
dif si - sf
if (dif = 0.15 and dif = (0.20+ increment))
and (reliability(i ) > 0.5)
then
K K + i
increment increment +0,5;
  until |K|>25;
end
}
```

The pseudocode above shows the risk retrieval process adopted, where X stands for the risk case group which represents the risk knowledge of a determined activity that exists within the knowledgebase of the risk mitigation system, mp represents the vector of attributes that describes the risk case, sf is the final risk mitigation solution generated in the measurement agent as a risk solution to the risk case, si is the solution to risk case i and K is the set of the most relevant risk retrieved cases [32].

4.3 Risk mitigation system agents and algorithm

This section shows the risk mitigation architecture system. The architecture illustrates how software agents and knowledge mapping are used for making decisions for mitigating risk in IT organization. The risk mitigation model has been developed using software agents and knowledge mapping as stated seven agents are incorporated to assist in decision making in mitigating operational and technical risk in IT organization [36]. Figure 5 shows the risk mitigation system architecture for making risk decision to mitigate risk in IT organization. The system architecture in Figure 5 of this paper is used to implement the risk mitigation system (RMS).

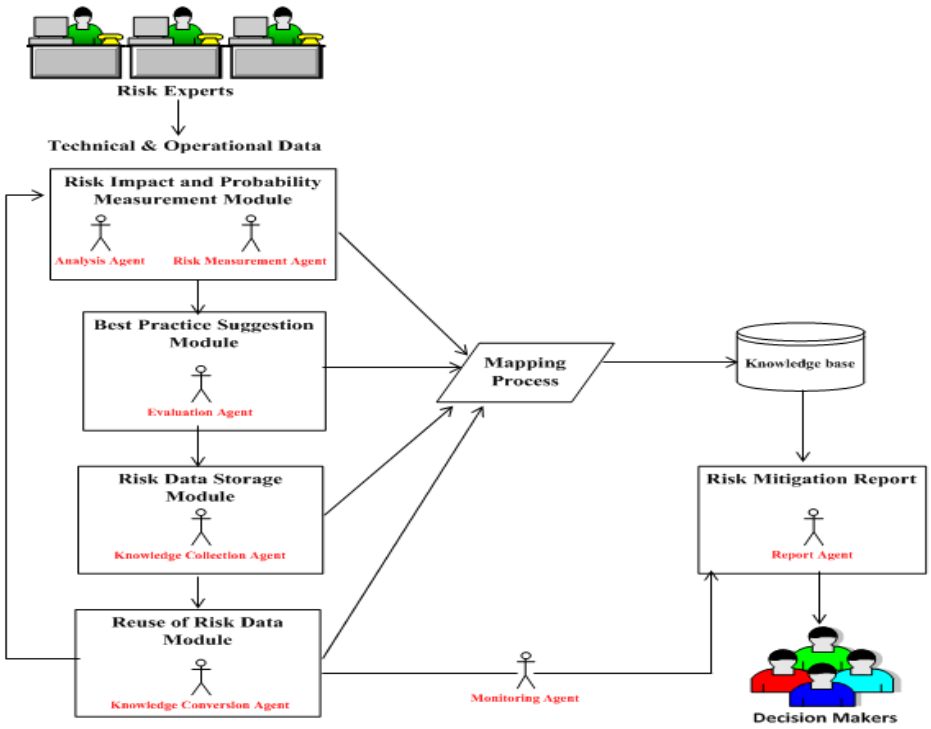

Figure. 5 Risk mitigation system architecture

Figure 5 shows the developed system architecture used to implement the risk mitigation system

4.4 Risk mitigation system architecture

4.4.1 Risk impact and probability module

a) Analysis agent

The analysis agent assist in analyzing the operational and technical risk base on the experts experience and skills on lesson learnt and best practices. The algorithm of the analysis agent is shown below.

Algorithms for analysis Agent
Analysis Agent, Knowledgebase, Expert, Risk

Algorithm analysis agent (val Risk < Expert >)
Step1: Pre- Knowledgebase is meta data structure to a valid Knowledgebase
Post- Knowledgebase risk status
Step2: Return: Boolean, false: Risk Knowledgebase empty;
Else true: Risk Knowledgebase contains data
Step3: If (Risk details not new)
Result = false
Else Result= true
Return result of Risk Knowledgebase
End empty Risk Knowledgebase

b) Measurement agent

The measurement agent assist in measuring the risk based on the risk impact and risk probability. This agent assigns different colors on the risk based on the measurement of the risk. The measurement agent saves the result of the measured risk to assist the practitioners in risk decisions in mitigating both operational and technical risk in IT organization.

Algorithms for Measurement Agent
Agent RiskMeasurement (K, P, I)
K Knowledgebase; P Risk Probability; I Risk Impact
RISK information to be measured by the measuring agent.
Step1 :{ Measures the risk probability}
If P=0 then
Printf ('This operational or technical risk cannot be measured')
Return
Step2 :{ Measures the Impact of the risk}
RISK=K [I]
Step3 :{ If impact is also 0, set risk probability and risk impact to 0}
If P=I then
R=low
If P=>I then
R= Medium
If P>1 & I> 1 then
R= High
{Otherwise measuring agent will reverse the Comparism}
Else
If I=P then
R=low
If I=>P then
R= Medium
If I>P & P> 1 then
R= High
Return (RISK)

4.4.2 Best practice suggestion module

a) Evaluation agent

Evaluation agents retrieves the risk impact and risk probability results from the risk measurement agent and also retrieves the best practices on how to mitigate the identified risk.

Algorithms for Evaluation Agent
Evaluation Agent (E)
K Knowledgebase, R Risk Evaluation Result
Step 1: Evaluation Agents stores the risk evaluation details

```
{Check for Knowledgebase if risk already exists}
If R=K then
Printf ('Risk already exist in knowledge')
Printf ('Do you wish to add risk evaluation comment')
Return
Step 2 :{ Increment risk pointer details}
(R=R+1 [K])
Step 3: {Check Risk values}
If R<0
Print ('Risk is has been stored in knowledgebase')
Step 4: Evaluation Agents retrieves the result
{display Risk Evaluation values}
For K value E to R
Print (R [K])
R=R+1
Return (E)
```

4.4.3 Risk data storage module

a) Knowledge collection agent

This agent retrieves risk data from the knowledgebase for the practitioners to mitigate risk.

```
Algorithms for Knowledge Collection Agent
Agent KnowledgeCollection (K, SIZE, F-Agent, R-Agent, RISK)
K    Agent
SIZE Knowledgebase size
F front Risk
R rear Risk;
RISK operational or technical risk to be added at the rear of risk table.
Step1 :{ Check risk knowledgebase status}
If R= = k>SIZE then
        Printf ('Knowledgebase is full')
        Return
Step2 :{ Increment rear risk}
k=R-F+1
Step 3 :{ Add new risk information at rear end of Knowledgebase risk table}
K=R+1
Step 4 :{ If initially, the knowledgebase is empty, the agent adjust the front r=Risk}
        If F =0,
then
Return (Risk)
Printf
('Knowledgebase is empty, operational or technical risk data can be added, Please Proceed')
```

4.4.4 Reuse of risk data module

a) Knowledge conversion agent

The knowledge conversion agents mainly convers the data from the MySQL knowledgebase to the HTML format for the practitioners, in making risk decisions for mitigating risk in IT organization. The looping of the risk is used to arrange the risk in the knowledge base, once a new risk is added by the expert the knowledge base is restructured and the new risk is added at the front of the risk list in the knowledge base. If the risk is searched the knowledge conversion agent converts and displays the newest risk in the risk list based on which list is added last.

Algorithms for Knowledge Conversion Agent
Algorithm for Knowledge Conversion agent queue (ref risk <metadata>)
Step 1: Pre- risk is metadata structure to a valid risk
Checks to be sure that the risk knowledgebase is not empty
If
Knowledgebase is not empty
Step 2: Proceeds to retrieve (risk.front not null)
risk.front = risk.front->next
Convert (risk format)
Step 3: End conversion
risk.front = 1
Then
Printf
('Risk Report Successfully Generated')
Else
Printf('Knowledgebase is empty')
Return
End risk report conversion

4.4.5 Risk decision module

a) Risk monitoring agent

The monitoring agent updates the practitioners involved in mitigating the risk, by automatically sending email update notification on the particular risk once any practitioners adds new information on the risk. The monitoring agents makes sure new risk data are added to the risk report, to aid risk decision in mitigating risk in IT organization.

Algorithms for Risk Monitoring Agent
Algorithm is Monitoring agent (val Email<Risk>) system users
Step 1: Risk mitigation data is in Knowledgebase
If Risk is been treated; System sends initial risk report
System Select expert user
Printf
('Initial Risk Treatment Status Successfully Sent')
Return available risk report;
Step 2: If (risk treatment successfully implemented)
Email Result = true
Printf
('Risk Treatment Update Successfully Sent')
Step 3: Else if expert user adds new risk comment
Return Send email risk comment result
Printf
('Risk Comment has been added')
Else Step 4: If no new risk update
Return existing report

b) Risk report agent

The report agent converts the HTML report the practitioners view in his/her computer or device and generates a PDF file format of the report using JavaScript for risk decision in mitigating risk. The risk mitigation system has been developed using software agents and knowledge mapping.

Thus, seven agents are incorporated to assist in decision making in mitigating operational and technical risk in IT organization. Figure 5 shows the risk mitigation system architecture for making risk decision to mitigate risk in IT organization. Below are the modules and risks agent in the system architecture, the software agents communicate and works together, providing support to practitioners in risk decision in mitigating risk.

Algorithms for Risk Report Agent
Agent GenerateRiskReport (R)
R Agent
Step1: {Check risk mitigation information values}
If Risk Data<0
Print ('There is no Risk Report on the Knowledgebase')
If Risk Data>0
Step2 :{ There is existing Risk Information, display Risk information values}
For R
Generate Report Value F-Report to R-Report
Print (R)
Return existing report
R= R+1

Other components of the system architecture include;

4.4.6 Knowledge base

Provides adequate support in the reuse of lessons learnt, best practices knowledge from previous projects to provide assistance and expertise in an effective way to mitigate risk. This knowledge can be useful to team members who are not familiar with current risks; the knowledgebase is quantified using opinions of experts. Less-experienced users can benefit from access to this expertise. The knowledgebase contains a knowledge map. The knowledge map shows which knowledge is used, this knowledge is useful for what risk, what is its relationship with other knowledge. The knowledgebase also updates and edits the knowledge by removing the outdated knowledge and collecting the feedbacks of decision makers about the application of knowledge in their decision [36].

4.4.7 Experts/operational/technical data

This is the risk data (tacit knowledge) that the experts add in to the risk mitigation system. This knowledge is stored in the knowledge base and used for future risk mitigations in IT organizations [36].

4.4.8 Decision makers

These are the practitioners i.e. decision makers, staff, managers or stakeholders that use the system to search for risk by sending a request. The decision makers send the request in a browser such as Internet explorer by using the query interface by clicking on the search button to confirm the information that the user entered in the query form, report agent sends the requests to the knowledgebase and translates this request into PDF documents (explicit knowledge) [36].

4.4.9 Mapping process

The mapping technique involving storing data into the knowledge base, and is responsible for its database maintenance. Knowledge Mapping is used in this process to store risk mitigation strategies in knowledge base. It may update existing knowledge which is outdated and not in use and also can remove the knowledge that is determined by experts. With use of knowledge map, agents can retrieve relevant knowledge for decision makers more effectively, because the knowledge map shows the relationship between knowledge and their usage. A knowledge map provides indexes to real knowledge, whether it is an actual map, a cleverly constructed database. It is a guide like Yellow Pages that shows where to find resources and knowledge. The knowledge map transforming tacit knowledge into explicit knowledge. Such transformation can clearly display tacit knowledge by texts, categories, and graphics. Because the knowledge mapping is a method of knowledge expression and a mechanism of knowledge storage, applies the mind mapping to build a knowledge map that can be easily understand by staff and management in the organization [36].

4.4.10 RMS interface

This phase in the software development life cycle (SDLC) involves the coding, deploying and running of the risk mitigation system (RMS) in XAMPP server locally to test the system to ensure the system is operational. This phase ensures that the system can assist practitioners in risk decision in mitigating risk in IT organization, thus this section

show how risk decision is being carried out for mitigating risk in IT organizations. The identified risk decision process; Measure risk impact and probability, suggest best practices, stores risk data and reuse risk data. The implemented risk mitigation system (RMS) is based on this process. Based on Figure 2 in this paper, the risk decision process is assists to provide support to practitioners in making decision on what action to take in mitigating the identified risk.

4.4.11 Measure risk impact and probability

To mitigate operational and technical risk, the risk experts adds the operational and technical risk that occurs in the organization such as computer crash, software failure or error, malware attack, communication infiltration, social engineering attack, technical failure, theft, misuse of system resources etc. These risks are added in to the enterprise knowledge base by the knowledge mapping process. The expert also selects the risk impact and probability scale, as shown in Figure 6 and Figure 7 and then the measurement and analysis agent measures the risk impact and probability of the risk and assigns color to the risk impact and probability based on the risk rating entered by the experts.

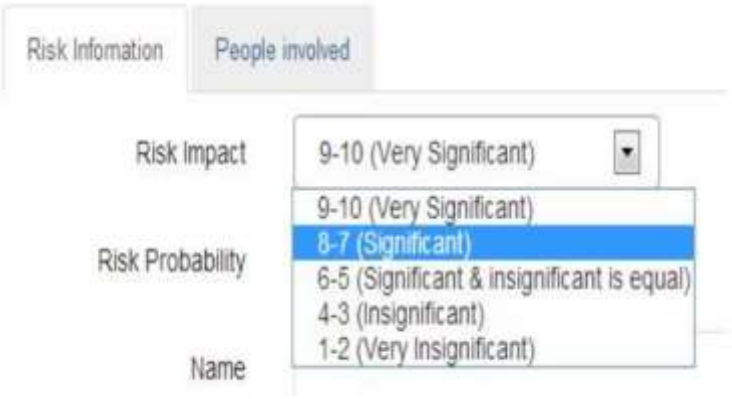

Figure. 6 Risk impact selection

Figure. 7 Risk probability selection

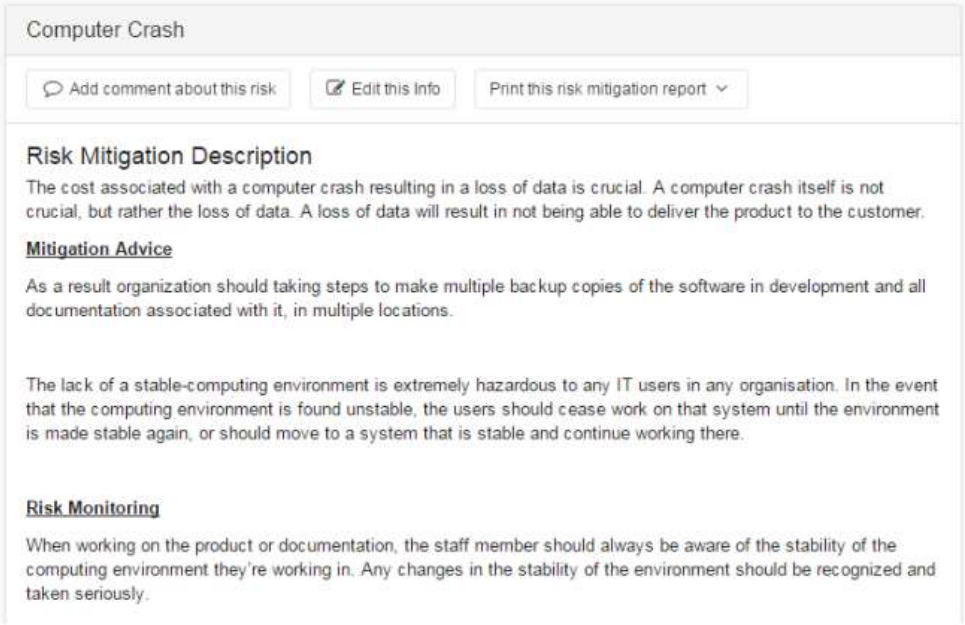

Figure. 8 Measurement and analysis agent measures risk

The best practices on previous risk mitigation are carried out by risk experts and are mapped and stored in the knowledge base. Thus, current practitioners can search for the information on how to mitigate risk and apply this knowledge in mitigating present operational and technical risk as seen in Figure 9.

ID	Name	Risk Impact	Risk Probability
27	Social Engineering attacks	9-10 (Very Significant)	9-10 (Very likely to occur)
28	Technical failure	6-5 (Significant & insignificant is equal)	8-7 (Will probably occur)
29	Theft	8-7 (Significant)	6-5 (Equal chance of occurring or not)
30	Misuse of system resources	1-2 (Very Insignificant)	1-2 (Very unlikely)
31	Staff shortage	4-3 (Insignificant)	4-3 (Probably not occur)
32	Wilful damages	1-2 (Very Insignificant)	4-3 (Probably not occur)
33	Disasters	9-10 (Very Significant)	8-7 (Will probably occur)

Figure. 9 Best practice suggestion

4.4.12 Best practice suggestion

The best practices are stored in the knowledge base. Knowledge collection agent assist in mapping practitioners search strategies on how to mitigate and reduce operational and technical risk, utilizing the risk mitigation system (RMS) as shown in Figure 10.

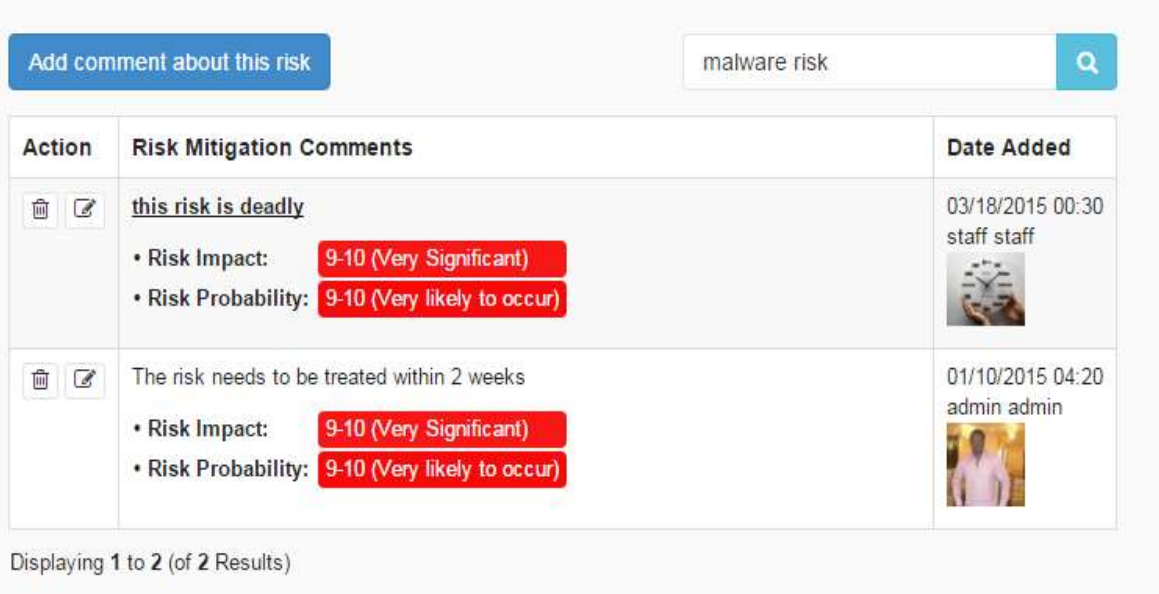

Figure. 10 Risk comment for best practice suggestion

4.4.13 Reuse of risk data

The reuse of risk data assists practitioners to download E-Report, containing information on how to mitigate and reduce operational and technical risk. The report comprises of the risk impact, risk probability and other risk mitigation information that is used for making decision on how to mitigate the risk.

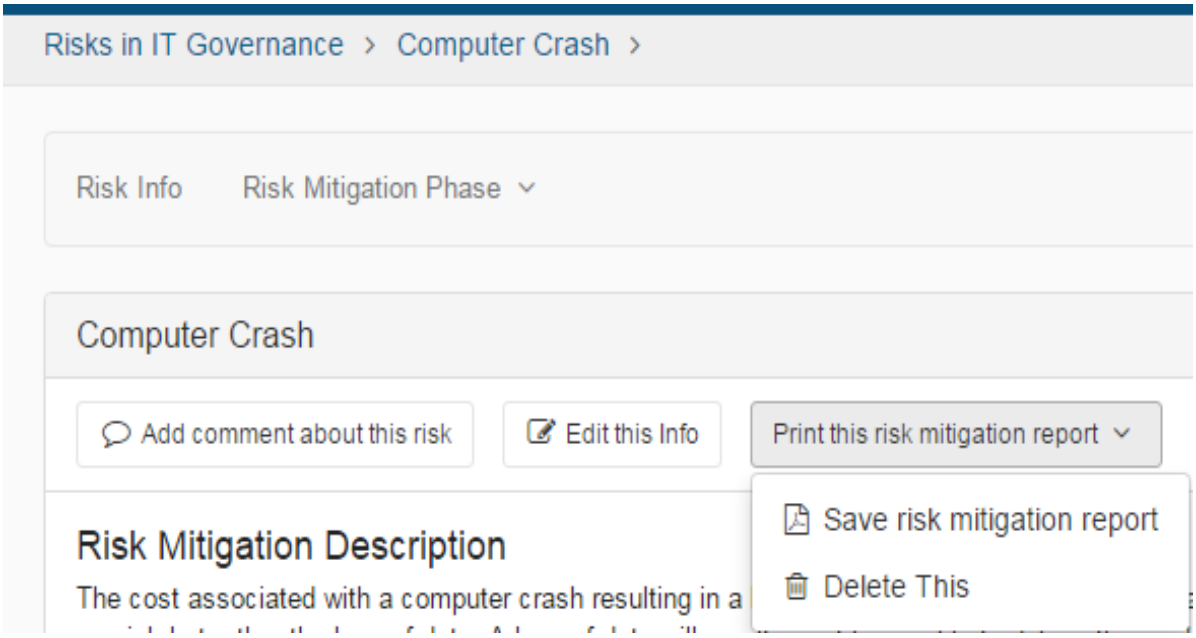

Figure. 11 Reuse of risk data for decision making

4.4.14 Risk report for decision making

Figure 12 shows the interface of the risk report. This module shows the information on the identified risk treatment is to be carried out using reuse concept via reuse of risk data. The data from the knowledgebase is converted to the HTML format for the practitioners, in making risk decisions for mitigating risk.

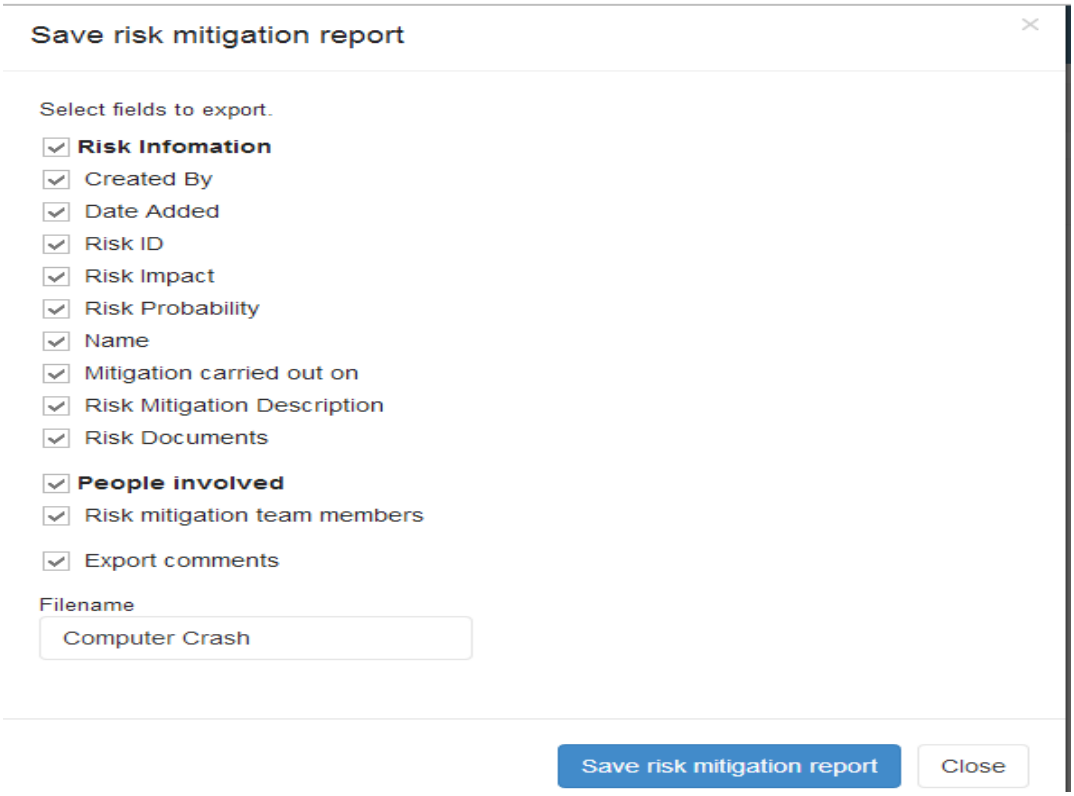

Figure. 12 Risk report for risk decisions for mitigating risk

5. DISCUSSION AND CONCLUSION

The developed risk mitigation system architecture in Figure 5 was used to implement the risk mitigation system (RMS). SDLC methodology was used to develop the agent bases risk system. The RMS was developed using probability and impact matrix to assist the agents in measuring the risk to provide support to practitioners in making risk decision relating to risk mitigation in IT organization. The system development methodology (SDLC) was followed in developing the risk mitigation system (RMS) to provide support to practitioners in risk decision for mitigating risk. The SDLC process involves requirement analysis, system design, implementation, testing and evolution. The risk mitigation tool was programmed using PHP MYSQL, for the agent and knowledgebase development and JavaScript for developing a usable and robust system. MySQL with TCP/IP network protocol is used to connect the risk knowledgebase with PHP using knowledge mapping process. The risk measurement component is called to access necessary information from knowledgebase, such as the probability and impact of each risk descriptions, to show the magnitude of the risk. The prototype allows experts to store and manage data on the system, by analyzing potential risk and its description and show potential risk mitigation result for each risk.

Thus, the RMS tool has been developed in order to tackle the limitations of the existing risk mitigation tools. The risk mitigation system produces risk reports for risk communication and risk tracking in a user-friendly and has in-built flexibility for re-configuration in a platform independent and provides user control over system inputs. RMS caters mainly for mitigating risk, since existing tools don't establish mechanisms for mapping and storing risks treatment process related to IT process for continuously update the knowledge to be gathered. The tool produced results during risk decision phase by providing support to decision makers. Therefore, RMS is developed to identify measure, treat and provide support to practitioner in mitigating perceived operational and technical risks that occurs in IT organization.

The core of the research is the reasoning methodology 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. Therefore,

RMS aims to provide a systematic approach to mitigate potential risk in IT organization, thus preventing system failures to occur. It is designed to be used as a decision support tool for decision-makers, such as practitioners, IT expert and management. RMS tools possesses the capabilities to support practitioners in mitigate risks, the tools can capture and reuse the lessons learnt from previous experience and best practices, to utilize and share the previous as well as existing knowledge and experience to assist in decision making via the mapping of knowledge. Future works involves extending the research to other organizations and mitigating more risk such as strategic risk, environmental risk etc.

ACKNOWLEDGEMENT

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

REFERENCES

1. Noraini, C. P., Bokolo, A. J., Rozi, N.H. N. and Masrah, A.A. M. 2015. A Review on Risk Mitigation of IT Governance. Information Technology Journal. 14(1). 1-9.
2. Junchao, X., Osterweil, L. J., Chen, J., Wang, Q. and Mingshu, L. 2013. Search Based Risk Mitigation Planning in Project Portfolio Management. ICSSP', 2013, May 18–19. 146-155.
3. Seung, H. H., Kima, D. Y., Kim, H. and Jang, W.S. 2008. A web-based integrated system for international project risk management. Journal of automation in construction. 9 (26). 342 – 356.
4. Khoo, Y. B., Zhou, M. and Kayis, B. 2005. An agent-based risk management tool for concurrent engineering projects. Complexity International Journal. 12(1). 1-11.
5. Kayis, I. B., Zhou, M., Savci, S., Khoo, Y.B., Ahmed, A., Kusumo, R. and Rispler, A. 2007. IRMAS – development of a risk management tool for collaborative multi-site, multi-partner new product development projects. Journal of Manufacturing Technology Management. 18 (4). 387-414.
6. Jabiri, K. B., Magnussen , C., Tarimo, C. N. and Yngström, L. 2008. The Mitigation of ICT Risks Using Emitl Tool: An Empirical Study. IFIP TC-11 WG11.1 &WG 11.5 Joint Working Conference, 157-173.
7. Saint, G. R. 2005. Information Security Management Best Practice Based on ISO/IEC 17799. Information Management Journal. 39 (1). 60-66.
8. ITGI. 2004. COBIT 3rd edition. Executive Summary, USA.
9. Jakub, M. and Janusz, G. 2001. Software support for collaborative risk management. Proceeding of 8th International Conference on Advanced Computer Systems, October 17-19, 2001 Mielno, Poland, 1-9.
10. 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.
11. 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, 7(1). 2072-2082.
12. 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.
13. Ahdieh, S. K. and 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.
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. 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.
16. Ahdieh, K., Hashemitaba, N. and Ow, S. H. 2014. A Novel Model for Software Risk Mitigation Plan to Improve the Fault Tolerance Process. IJITCM. 1(1). 38-42.
17. 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.
18. Xu, R., Pei, Y. N. S., Ying, L. H. Q. and Yun, T. L. 2005. Optimizing Software Process Based On Risk Assessment and Control. Proceedings of the 2005 the Fifth International Conference on Computer and Information Technology, 1–5.
19. Emmanuele, Z., Bolzoni, D., Etalle, S. and Salvato, M. 2009. Model-Based Mitigation of Availability Risks. IEEE Conference, 75-83.
20. Ayad, A. K. and Hashim, K. 2000. A model and prototype tool to manage software risks. IEEE international conference, 297-305.

21. Michael, R. L., Jinsong, S. Y., Keramidas, E. and Dalal, S. R. 1995. ARMOR: Analyser for Reducing Module Operational Risk. IEEE Conference, 137-142.
22. Thamer, A., Sulaiman, S. and Salam, R. A. 2009. Project Management Using Risk Identification Architecture Pattern (RIAP) Model: A case study on a Web-based application. 16th Asia-Pacific Software Engineering Conference, 449-456.
23. Rajes, S. H. and Alexander, S. M. 2009. Application of Web Based Supplier Risk Assessment for Supplier Selection. Proceedings of the 2009 Industrial Engineering Research Conference, 2259-2264.
24. Gulcin, Y., Cebi, S. Hoegec, B. and Ozok, A. F. 2011. A fuzzy risk assessment model for hospital information system implementation. Expert Systems with Applications. 39(1). 1211–1218.
25. Pratim, D. and Acar, W. 2010. Software and human agents in Knowledge Codification. Knowledge Management Research and Practice. 8(1). 45-60.
26. Suresh, R. H. and Egbu, C. O. 2004. Knowledge mapping: concepts and benefits for a sustainable urban environment. 20th Annual ARCOM Conference, 905-916.
27. Gangcheol, Y., Dohyoung, S., Hansoo, K. and Sangyoub, L. 2011. Knowledge-mapping model for construction project organizations. Journal of Knowledge Management. 15(1). 528–548.
28. Ali, S. S. B. Masoumeh, Z. and Mohd, Z. A. R. 2014. A Comprehensive Review of Knowledge Mapping Techniques. Journal of Information Systems Research and Innovation. 1(1). 71-76.
29. John, D., Isaac N. and Admire, K. 2009. Intelligent Risk Management Tools for Software Development. SACLA, ACM, 33-40.
30. Mihalis, G. and Michalis, L. 2011. A multi-agent based framework for supply chain risk management. Journal of Purchasing and Supply Management. 3(1). 23–3.
31. Fu, R., Yue, X., Song, M. and Xin, Z. 2008. An architecture of knowledge management system based on agent and ontology. The Journal of China Universities of Posts and Telecommunications. 15(1) 126–130.
32. Javier, B., María, L. B. Juan, P., Juan, M. C. and María, A. P. 2012. A multi-agent system for web-based risk management in small and medium business. Journal of Expert Systems with Applications. 39(1). 6921-6931.
33. Shikha, R.. and Selvarani, R. 2012. An Efficient Method of Risk Assessment using Intelligent Agents. Second International Conference on Advanced Computing and Communication Technologies, 123-126.
34. Noraini, C. P., Bokolo, A. J., Rozi, N. H. N. and Yusmadi, Y. J. 2015. 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, 737-742.
35. Bokolo, A. J. and Noraini, N. C. 2015. A Review on Tools of Risk Mitigation for Information Technology Management. Journal of Theoretical and Applied Information Technology. 11(1). 92-101.
36. Bokolo, A. J., Noraini, C. P., Teh, M. A., Rozi, N.H. N. and Yusmadi, Y. J. 2015. Autonomic Computing Systems Utilizing Agents for Risk Mitigation of IT Governance. Jurnal Teknologi. 77(18) 49-60.

AUTHOR PROFILE