Jurnal
Teknologi

Full Paper

AUTONOMIC COMPUTING SYSTEMS UTILIZING AGENTS FOR RISK MITIGATION OF IT GOVERNANCE

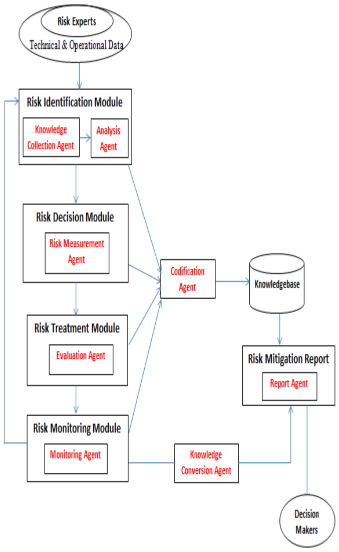
Bokolo Anthony Jnr, Noraini Che Pa*, Teh Noranis Mohd Aris, Rozi Nor Haizan Nor, Yusmadi Yah Jusoh

Faculty of Computer Science and Information Technology, University Putra Malaysia, 43400 UPM, Serdang, Selangor, Malaysia

Article history
Received
15 May 2015
Received in revised form
1 July 2015
Accepted
11 August 2015

*Corresponding author
norainip@upm.edu.my

Graphical abstract



Abstract

Risk mitigation has gained relevance during the last years and has helped to solve risk and improve decision making among decision makers in IT Governance. However, there is still a increasing need of developing innovative tools that can help IT Practitioners to solve risk in IT Governance. Existing risk mitigation approaches or tools lacks need for adequate data which is very important in mitigating risk and there is difficulty of mitigating risk generally in IT Governance. This paper present an autonomic computing model developed to mitigate risk; mainly operational and technical in IT Governance by measuring the risk and providing risk report to the management and staffs in organisations. Autonomic Computing Systems (ACSs) are systems that manage themselves. The core of Autonomic Computing Systems are type of agent with advanced capacities for reasoning to measure the risk probability and risk impact based on available data in the knowledge base or previous experiences. The Autonomic Computing Systems provide risk advice aimed at providing decision support to management hence mitigating risk in IT Governance. Data was collected via purposely sampling using interview by case study among 13 Malaysia universities. The data was analyzed by Nvivo to get an insight on the current risk mitigation practices and process, after which a risk mitigation model has been developed using autonomic agents.

Keywords: Software autonomic computing, risk, risk mitigation agents, & IT governance

1.0 INTRODUCTION

Risk can be defined as the possibility of suffering loss. In IT Governance the loss could be in the form of diminished efficiency of the IT system; (operational risk), increased maintenance costs, delayed completion, or failure in the IT infrastructure (technical risk) [1]. Nowadays is generally acknowledged that IT practitioners are in charge for mitigating the risks associated in utilizing IT infrastructures. IT Governance has emerged as a support for IT practitioners, as an important part of management's striving efforts to perform better in a competition environment. IT Governance can be said to be procedures and policies established in order to assure that the IT system of an organization sustains its goals and strategies [2]. Risk mitigation enhances organisation performance by helping the management discharge its duties facilitating efficient, effective and entrepreneurial management that can deliver value over the longer term. Risk mitigation offers the grounds for creating a complete and coherent integrated mitigation system, by generating efficient risk treatment strategies. This process reinforces any organization's corporate management, by taking into account the existing technological infrastructure, the adopted control strategies and investment solutions [3].

Risk mitigation involves the application of appropriate tools and procedures to solve risk within acceptable limits by identifying the risk, making risk decisions, treating and eliminating potential risk and monitoring the risk. Continuous Risk Mitigation is IT

Governance practice with processes, methods, and tools for solving risks. It provides a disciplined environment for proactive decision-making to assess continuously what can go wrong (risk); determine what risks are important to deal with; implement strategies to deal with the risks. Risk mitigation aims at early identification and recognition of risks and then actively changes the course of actions to mitigate the risk [1].

In utilizing IT infrastructures such as hardware, software and network facilities operational and technical risk occur. These risks need to be mitigated so that the organisation can function properly and achieve its objectives. There is the need for a risk mitigation tool or process; therefore the researchers propose a multi agent based model to mitigate in IT Governance. The model is enhanced by the agents' ability to measure the risk based on the risk probability, risk impact and degree of data sharing and reuse as well as the available risk report support for decision making processes within IT Governance. These risk report are useful in supporting decision making processes and augmenting critical dependencies between operational and technical risks which are in turn used as feedback to risk analysis processes, hence creating the iterative nature of risk mitigation processes. The risk report assists in risk monitoring which is a continuous process of supervising the entire process of risk mitigation. It constantly monitors the existing risk and suggests risk advice.

The aim of Autonomic Computing (AC) is to improve the risk mitigation system abilities by monitor data sensed by multi agents, analyzing the risk data, and adjust their operations according to policies, thus reducing complexity. Some benefits of autonomic computing include reduction of costs and errors, improvement of services, and reduction of complexity. An ACS is a system that manages itself. AC is emerging as a method to the design, development, and management of large scale distributed risk computing systems. Autonomic computing and software agent technology are viewed as new technologies to solve risk and enhance the design, implementation, and the mitigation of risk in IT Governance [4]. The agents have autonomous behavior and make decisions according to predefined policies. Each change in behavior of an agent can create instabilities in the entire system, because that agent can affect other agents. Software agents can be viewed as autonomic elements and this means that agent-oriented architecture can help for the implementation of self-risk mitigation systems [4].

In mitigating risk in IT Governance it is relevant to provide innovative and decision support tools that can assists in treating risk. These tools and methods can contribute to improve the existing business control mechanisms, solving the risk by predicting undesirable situations and providing recommendations based on previous experiences. However, mitigating risk in IT Governance tends to be a complicated process. The use of multi-agent can be an alternative risk treatment and decision making tool for collaboration within IT Governance risk mitigation [5].

In computer science, an agent can be defined as software entity, which is autonomous to accomplish its design objectives, considered as a part of an overall objective, through message communication and coordination with other agents. Thus risk mitigation processes can be perceived as facilitated by several autonomous decision making entities (software agents), each responsible for specific activities and performing different roles. These agents interact and cooperate with other agents, within and across organizations, in order to solve problems beyond their individual knowledge or expertise, and to promote a higher performance for the entire system [6].

The aim of this paper is to present a multi-agent risk mitigation model. The structure of this paper is organized as follows: section 2 presents the related works. Section 3 describes the methodology used in this research Section 4 describes the multi agent based risk mitigation model of the study. Section 5 is the discussion and conclusion section. Finally section 6 is the conclusion presented by the researchers.

2.0 RELATED WORKS

Autonomic Computing has gained world attention in recent years for the reason of developing applications with self-managing behaviour. Automatic computing requires advances in several fields such as software architecture, learning and reasoning, modelling behaviour, policies, multi-agent systems, and knowledge base design. As a consequence, there is a need for systems which address these problems, work independently of humans, and manage themselves according to a set of goals such as mitigating risk in IT Governance [4]. Risk is a potential problem it might happen or it might not. But, regardless of the result, it's a good idea to identify it, review its probability of occurrence, estimate its impact, and set up a mitigation plan. Risk mitigation process involves risk identification, risk decision, risk treatment and risk monitoring by coordinating and economizing application of resources to solve, monitor the probability and/or impact of the risk. In IT Governance risk mitigation aims at early identification of risks and then actively changes the course of actions to mitigate the risk [7].

[5] developed a multi-agent web based risk management system mentioning that multi-agent systems are the most leading solution to risk mitigation distributed systems. Since agents are computational entities that can be characterized through their capacities in areas such as autonomy, reactivity, pro-activity, social abilities, reasoning, learning and mobility. These capacities make the multi-agent systems very appropriate for constructing risk mitigation systems [5].

[7] presented an intelligent knowledge management decision making risk tool composed of

groups of agents which interact with each other to achieve their goals. Due to the social interaction factor, a multi-agent system is ideal for modelling the basic issues where interaction, interdependence, emergence, and conflicting interests are necessary. The researcher proposed that multi-agent system can extract, produce, store, retrieve, present and update the related knowledge in support of risk mitigation decision making [7]. [6] proposed a multi agent based framework for supply chain risk management by highlighting mitigation strategies for different types of risks. They mentioned that agent based technology is acknowledged as one of the most promising technologies for effective risk management and mitigation. The researchers mentioned that through their learning capability, multi agents can demonstrate efficiently the proactive and autonomous behaviour of the participating agents in mitigating risks. They can also promote a high level of cross organizational collaboration in a computational and cost efficient manner [6].

[8] presented a multi agent based virtual enterprise risk system to provide support for decision makers. The application of agent technology can reduce the labour intensity of the work involved in information management. Therefore, the system can also provide decision support for policy makers. In order to require the ability to learn using agents can improve system performance. The system model comprises of four components namely risk data management, risk task management, coordination and online monitoring. Risk data management is responsible for the risk information collection, sorting and storage. It includes risk identification, information conversion and risk assessment sub-modules [8].

[1] developed an intelligent risk assessment and management tool for software development. The goal of the tool is to enable engineers, managers, and other decision makers to identify, sufficiently early, the risks associated with software acquisition, development, integration, and deployment so that appropriate management and mitigation strategies can be developed on a timely basis. The tool assists in software process by in cooperating intelligent agents that carryout risk prevention, risk mitigation and correction and ensure safe system failure. The tool requires the ability to learn, to acquire knowledge and then use the knowledge to effect a change in behaviour. Furthermore, the tool in future projects ensures continuity in the use of experience in risk management from previous projects. The tool fosters the application of the integration of formal methods and heuristic approaches to ensure support for the evaluation, comparison, analysis, and evolution of agent behaviour [1]. [9] presented an agent based risk management tool for concurrent engineering projects that supports project risk management as an iterative and continuous process across large-scale collaborative engineering teams throughout the lifecycle of projects. In particular, the researchers demonstrate how a flexible and extensible framework of agents is constructed to form an intelligent risk mapping and assessment system. The agent based tool is founded upon data sharing, group decision support (GDS), and agent-based concepts. The agent-based approach addresses these shortcomings by isolating business logic that changes frequently. In this approach, each agent is designed to be a dedicated software module that performs one specific task of the system. The tool was designed as an agent-based project risk mapping and assessment tool in a web-based project collaborative workbench that aims to support such requirements in addition to maintaining data consistency and coordination [9]. [10] designed a generic conceptual model of risk evaluation in order to manage the risk through related constraints and variables under a multi-agent collaborative design environment. The model used an intelligent data based reasoning methodology to deal with risk mitigation by combining inductive learning methods and reasoning consistency algorithms with feasible solution strategies. The effectiveness of the model aiming for risk mitigation in concurrent engineering (CE) projects is determined by the degree of data sharing and reuse, as well as the available support for decision making processes within the projects. The model comprises of an intelligent data-based reasoning methodology (IDRM) which is expanded to deal with risk mitigation by combining the inductive learning method and the reasoning consistency algorithm with feasible solution strategy. Consequently, the novel model will not only facilitate the decision making from a risk perspective but also emphasize on the data retrieving, storing, sharing and updating [10].

[11] proposed a method in risk assessment using intelligent agents during risk identification phase. The agent for risk identification is goal based agent which has goal information to explain desirable circumstances. The performance element consists such as the requirement specification, stakeholders' inputs, risk history and procedures which can handle each risk separately. The actions depend on the project which the agent is acting upon. When the agent is run for the first time, it will not have any entries in the risk history. The critic is also responsible for choosing between two risk mitigating methods for the same type of risk depending upon the estimated cost. 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 outdating. The problem generator identifies improvements for the existing procedures to handle risks by trying out various other possibilities of solving the same kind of risks [11].

2.1 Importance of Autonomic Computing Software Agents in Risk Mitigation

An ACS is a self-management system that can predict and prevent risk. Self-optimization is the capability of maximizing resource allocation and utilization for satisfying user requests. An ACS can identify and detect risk and cover all aspects of risk mitigation at different levels such as the platform, operating system, applications, etc. It can also predict risk based on sensor reports and attempt to avoid them. It is called self-protection. An ACS can know itself and is aware of its components, current status, and available resources. It also knows which resources can be borrowed or lent by it and which resources can be shared. It is self-awareness or self-knowledge property. An ACS is also aware of the execution environment to react to environmental changes such as new policies. It is called context-awareness or environment-awareness. Openness means that an ACS can operate in a heterogeneous environment and must be portable across multiple platforms. Finally, an ACS can anticipate its optimal required resources while hiding its complexity from the end user view and attempts to satisfy user requests. Self-configuration, self-healing, self-optimization, and self-protection are considered as major characteristics and the rest as minor characteristics that are suitable for risk mitigation using multi software agents [4].

A software agent can act as an interface between the user (decision makers, IT experts and IT practitioners) and the rest of the components of the system. Moreover, multi-agents can predict risky situations. Multi-agents collaborate and can evolve over the time and adapt to the changing conditions of the environment. Thus, making possible to detect risky situations in IT Governance and providing suggestions and recommendations that can help to avoid possible undesirable situations. Multi-agents system incorporate techniques to analyze the data from enterprises, extract the relevant information, and detect possible failures or inefficiencies in the operation processes [5]. According to [7] Multi Agent assist in retrieving risk knowledge based on its importance freshness and relation with problem and then shows this knowledge to user with high score from top to down. Second, it gets feedback from users about the application of extracted knowledge based on the risk. Third, multi-agents assist in updating the risk knowledge in knowledge base [7].

[7] added that multi-agents recovers information from previous experiences simplifies the prediction process by detecting and eliminating relevant and irrelevant patterns detected in previous risk mitigation. Thus providing a revise and retain stages to implement a decision support system for experts. Multi-Agents makes use of knowledge obtained from the risk experts. By providing recommendations to avoid risky situations and improving the overall functioning of IT Governance. Thus multi-agents have the ability to adapt to changes in the environment making use of past experiences. Thus the knowledge acquired when resolving new problems is used for future situations [7]. Multi-agents provide resources to minimize, monitor, and control the probability and/or impact of risk. Multi-agents in risk mitigation aim at early identification and recognition of risks and then actively changes the course of actions to mitigate and reduce the risk [11]. [1] added that use of agents in risk mitigation will foster and ensure support for the measurement, and treatment of risk [1]. [8, 9] stated that the application of agent technology, one can provide decision support and feedback for policy maker.

2.2 How Autonomic Multi Agents Communicates

Autonomic Multi-agent systems are composed of groups of agents which interact with each other to achieve their goals. Due to the social interaction factor, a multi-agent system is ideal for modelling the basic issues where interaction, interdependence, emergence, and conflicting interests are necessary. This communication ability of agents that lets agents work together makes a system which is called multi-agent system [7].

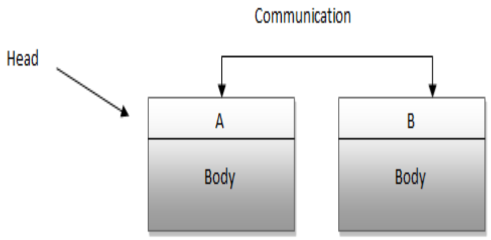


Figure 1 Schematic view of agents

The general architecture of each individual software agent, as shown in the Figure 1 includes body, head, and communication abilities The body contains all the centralized processes; they are the tasks given to each agent to accomplish which can be different, depending on their role. The head includes the information provided either from the user, environment or the other software agents and the communication ability includes all the functions required in order that the agents be able to communicate and as a result, to cooperate with other members of the agent society [7].

2.3 Characteristics of Autonomic Computing Multi Agents

[6] stated that agent based technology is acknowledged as one of the most promising technologies for effective mitigation of risk that are characterized by high levels of uncertainty due to its vital characteristics as indicated in Table 1.

Table 1 Characteristics of Autonomic computational software agents [a]

Characteristics	Description
1. Autonomy	Agents are aware of their environment operating without human intervention to some extent in order to mitigate risk [6]. Thus agents have capabilities of risk mitigation task selection, prioritization, goal-directed behaviour, decision-making without human intervention [1]. With autonomous behaviour, agents can take control over risk activities and work without human interference [7].
2. Social ability	Agents are able to engage other risk mitigation agent via communication and coordination; [6] they may collaborate on risk mitigation [1], Thus social ability enables agents to communicate with other agents or human operators [7].
3. Reactivity	Agents can perceive their environment and respond to specific risk mitigation changes in this system [6]. Agents perceive the context in which risk are mitigated and react to it appropriately [1]. Reactivity helps agents to react to risk changes that are in the environment [7, 12]
4. Pro-activeness	Agents do not simply respond to risk changes in their environment, but can initiate risk mitigation suggestions [6]. Thus agents should be initiative based on risk mitigation goals [7].
5. Persistence	Agent is not executed on demand but runs continuously and decides for itself when it should assist in risk mitigation [1, 12].
6. Intelligence	Agent can maintain a condition of balance or equilibrium within when mitigating risk, even when faced with external changes and assist in risk mitigation efficiently and expertly without assistance from human [12].
7. Mobility	This refers to an agent's ability to migrate from one process in a system to another in order to perform essential tasks such as risk identification [12].
8. Interactivity	Is another characteristic that marks the ability of an agent to maintain communication between different risk mitigation processes [12].

3.0 METHODOLOGY

Qualitative approaches were used for collecting data. Qualitative research is a means for exploring and understanding the meaning form individuals or groups ascribe to a social or human problem. The process of research involves emerging questions and procedures. In this research secondary data was collected from existing literatures on risk mitigation in IT, the data was synthesized and extracted following systematical literature review (SLR) conducted by the researcher. Primary data was collected employing case study by interview session on 13 Malaysian universities. First was the pilot study in which data was carried out using interview in 3 universities with 7 respondents to the test the instrument and to generalize the data for the main interview. Secondly the main interview session carried out in 10 Malaysian universities with 13 respondents using case study research approach.

Figure 2 shows the Research method that was used in the research. The research has 3 phase comprising of the literature review, the main study that involved data collection by open ended interview using case study and analysis of data using Nvivo, lastly the development of the autonomic risk mitigation model.

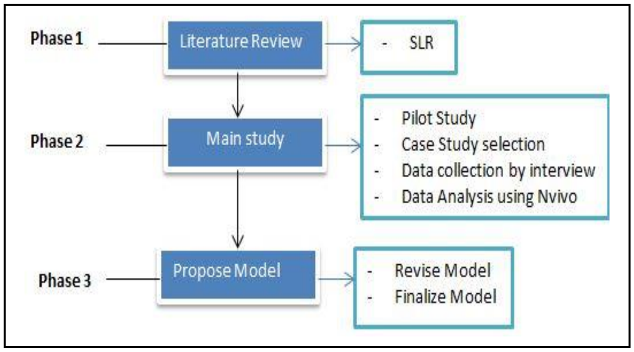


Figure 2 Research Method

3.1 Case Study

Case study was carried out involving in-depth investigation of IT practitioners in Malaysian Universities over a period in time. E.g. how they mitigate risk in their organisations. Data was collected using Case study by conducting open ended interview, mainly on IT practitioners and IT experts in 13 Malaysian universities. The case study is the combination of the data collected from the pilot and main data collection. The interview is considered open-ended because even though the questions can be scripted, the interviewer usually doesn't know what the contents of the response will be. The interview questions focus more on the participant's experiences, knowledge, skills, ideas and preferences on risk mitigation. The targeted population for this survey is experienced IT professionals that have in depth knowledge of risk mitigation and management. Additionally, it is assumed that the data derived from the responses given by this sample is sufficient to achieve the goal of developing a risk mitigation model in IT Governance. For sampling strategy purposely sampling is used, in which the respondents (IT practitioners and IT experts) for the interview are selected based on their idea, knowledge and experience in risk mitigation practices in various Malaysian universities.

3.2 Data Analysis

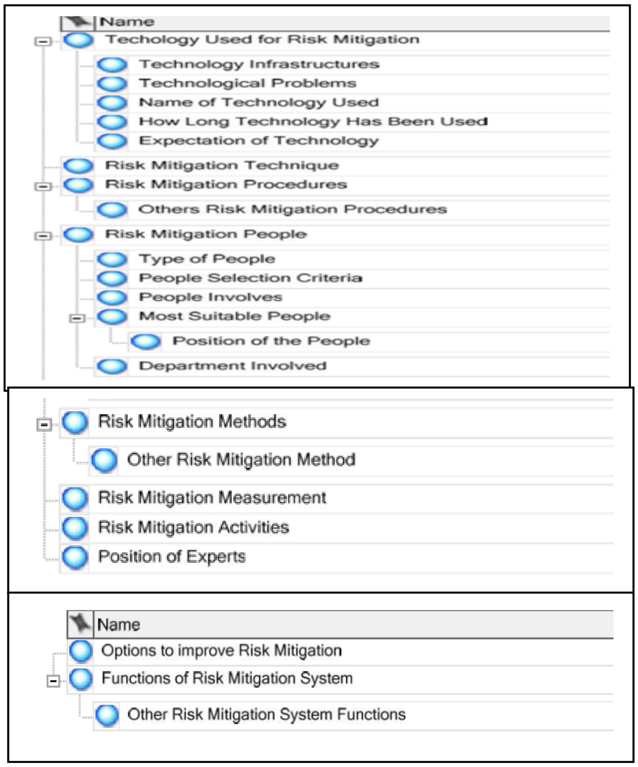
At the end of the data collection process 20 interview transcript was collected back from the 20 respondents from 13 various universities as showed in Table 2. The interview transcripts were analyzed using Nvivo software package in to categories, codes and notes based on the people involved in risk mitigation, technology used for risk mitigation (ranging from the hardware, software, network communication and other devices), the process, activities, procedures, methods and practices involved in risk mitigation.

Table 2 Data collection Respondent and position

Case Study	Respondents	Position
1.	1	IT Systems Analyst
2.	2	ICT Officers
3.	2	Network Administrators
4.	1	Head of IT Projects
5.	1	ICT Director
6.	2	ICT Managers
7.	1	IT Security Auditor
8.	1	Head of ICT unit
9.	1	Head of IT department
10.	1	Head of IT Unit
11.	1	Head of IT Security
12.	2	Heads of IT Unit
13.	4	IT Dept. Staffs

3.3 Results

Nvivo was used to analyze the interview transcripts in to categories and nodes as shown in Figure 3. The categories are explained briefly below;



Name
- Techology Used for Risk Mitigation
  - Technology Infrastructures
  - Technological Problems
  - Name of Technology Used
  - How Long Technology Has Been Used
  - Expectation of Technology
- Risk Mitigation Technique
- Risk Mitigation Procedures
  - Others Risk Mitigation Procedures
- Risk Mitigation People
  - Type of People
  - People Selection Criteria
  - People Involves
  - Most Suitable People
    - Position of the People
  - Department Involved
- Risk Mitigation Methods
  - Other Risk Mitigation Method
- Risk Mitigation Measurement
- Risk Mitigation Activities
- Position of Experts

Name
- Options to improve Risk Mitigation
- Functions of Risk Mitigation System
  - Other Risk Mitigation System Functions

Figure 3 Category and nodes from Nvivo

1. People

These are team members involve in the risk mitigation.

2. Technology

Comprises the software, hardware, network communication used for mitigating risk.

3. Techniques

Involves techniques that assist in risk mitigation such as Spread sheets, Focus group, discussions, Scenario analysis, Brainstorming, lessons learnt, Checklist, Risk breakdown, Inductive reasoning, SWOT analysis, Team Meeting, Worksheet lists.

4. Methods

Involves either qualitative or quantitative methods such as Interview, questionnaire, workshops, survey used for risk mitigation.

5. Management

The decision maker or management.

6. Risk Mitigation

This is the current risk mitigation process or software being used.

7. Procedures

This are the step-by-step sequence of events or course of action carried out in risk mitigation.

8. Activities

Refer to the condition in which risk is being carried out or how risk mitigation is being implemented in the organization.

9. Measurement

Risk mitigation values made meaningful by quantifying into specific units either by quantification or quantifying.

4.0 AUTONOMIC COMPUTING SYSTEM MODEL FOR RISK MITIGATION IN IT GOVERNANCE

Figure 4 shows the autonomic computing system based risk mitigation model using software agents;

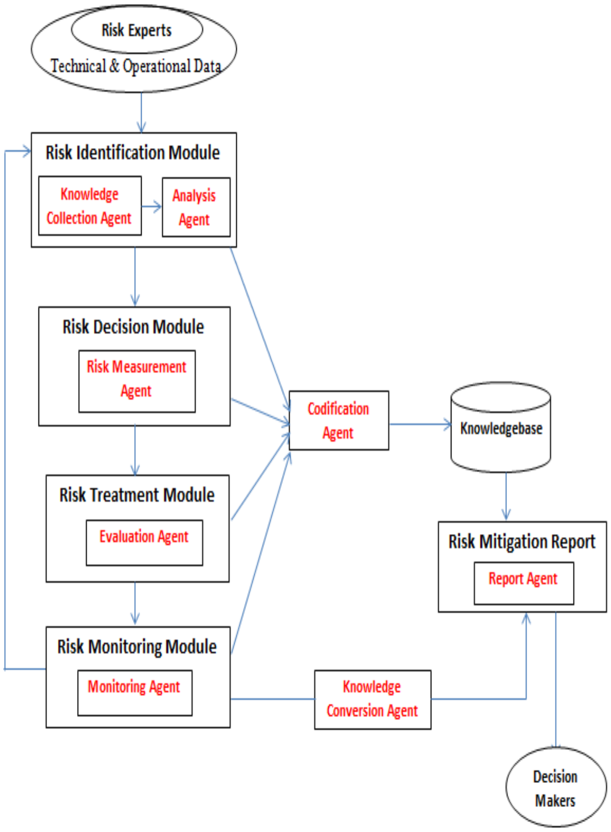


Figure 4 Autonomic computing system based risk mitigation model

4.1 Risk Mitigation Autonomic Computing Modules

Below are the risk mitigation autonomic computing modules;

1. Risk Identification

In risk identification potential risks are determined by IT practitioners by using process such as Risk Rating, Screening, Examination of risk drivers and assumption risk analysis. Risk identification is the first stage of the risk mitigation process. It is concerned with identifying the risks that could result to major threat to the project process. Risk identification may be a team process where a team get together to brainstorm possible risks [13].

2. Risk Decision

Risk decision helps the decision makers to estimate the impacts and probability 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, using process like decision tress or risk breakdown.

3. Risk Treatment

Risk treatment is defining an effective strategy to solve the risks associated with the various risk classes defined. In risk treatment, the management perspective is included in the treatment of IT risks by comparing various solutions to the risk using process such as Bench marking, Cost benefit analysis and Benchmark to state mission.

4. Risk Monitoring

Risk monitoring aids in the checking of the risk milestones as the risk treatment is applied using process like Knowledge Mapping, Standard risk management plan and Milestone tracking. Risk monitoring helps in reporting and reviewing of risks [9, 14].

5. Risk Mitigation Report

This module comprises of risk output retrieved from the knowledge base for the management and staffs in IT organisation. It comprises of the risk description, risk probability, risk impact estimation, mitigation advice/documentation and other information on how to treat IT risk [14].

6. Knowledgebase

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 [9]; [14]. Lessexperienced users can benefit from access to this expertise.

7. Operational/Technical data

This is the risk data (implicit 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 organisations.

8. Decision Makers

These are the staff, managers or stakeholders that use the system to search for risk by sending a request.

4.2 Reason for Implementing Autonomic Computing Agents for Risk Mitigation in IT Governance

Autonomic agent can act as an interface between the user and the rest of the elements of the intelligent environment. Moreover, agents can incorporate advanced intelligence models to predict risky situations in IT Governance. Agents collaborate to create models that can evolve over the time and adapt to the changing conditions of the environment. Thus, making possible to detect risky situations In ITG and providing suggestions and recommendations that can help to avoid possible undesirable situations. The core autonomic agent system are the analysis agents, that incorporate new techniques to analyze the data from enterprises, extract the relevant information, and detect possible failures or inefficiencies in the operation processes [5].

Through autonomic agent technology learning capability, they can demonstrate efficiently the proactive and autonomous behavior of the participating agents in mitigating risks in real time. They can also promote a high level of cross organizational collaboration in a computational and cost efficient manner. The inherent distributed nature of autonomic agent based technology (in that, a problem solution is distributed to different agents) gives the significant advantage of ease in dealing with the high level of complexity of ITG in contrast with conventional information technology.

[6] added that the interactions among these agents were subsequently modelled by analyzing several risk identification and mitigation processes. Autonomic agents make use to past experiences to resolve new problems, as such; it is perfectly suited for solving the problem at hand (risk mitigating). Autonomic agent specialized in detecting risky situations. The recovery of information from previous experiences simplifies the prediction process by detecting and eliminating relevant and irrelevant patterns detected in previous analyses. Moreover, the knowledge obtained during the prediction process is of great importance for subsequent predictions.

4.3 Risk Mitigation Autonomic Agents

There are several autonomic agents for risk mitigation such as knowledge collection agent, analysis agent, risk measurement and others. The details of the autonomic agents as indicated in Table 3.

Table 3 Autonomic Agents for Risk Mitigation

Agents	Description
Knowledge Collection Agent	The function of knowledge collection agent is to collect risk data. This agent is responsible for collecting tacit risk knowledge of experts. After collection, raw data is directly stored in the database.
Analysis Agent	This agent is responsible to collect experts' reasons and judging skill to ensure the best use of human understanding, since they have experience and knowledge about risk mitigation from past experience. This agent is responsible for retrieving new knowledge on how to mitigate risk in IT Governance. This agent finds expert users then connects to knowledge base. Then it retrieves new knowledge that may be of interest and are related to his/her expert. Finally this agent sends the new risk knowledge to the measurement agent. The analysis agent assists the measurement agent.
Risk Measurement Agent	The function of risk measurement agent is to measure the risk based on that which is specified by the experts. This agent uses the risk impact and probability for risk decision.
Evaluation Agent	Responsible for storing and releasing the evaluation results. When necessary, the data can be converted into a format required by the knowledge conversion agent.
Monitoring Agent	Monitoring agent constitutes risk warning information based on risk data, and passes the information to other modules. Monitoring agent applies the comments of stakeholders to assist in mitigating risk.
Knowledge Conversion Agent	Uses knowledge and rules of the expert system for risk decisions, then generates specific risk mitigation plan for each decision makers. Knowledge conversion agent recovers risk information in a user's query form, translates the user's request into visual documents, and sends the documents to report agent.
Report Agent	The report agent presents the needed risk mitigation knowledge to decision makers through interface. This agent filters, synthesizes and extracts risk knowledge from the information added by the experts.
Codification Agent	Responsible for storing data into the knowledge base, and is responsible for its database maintenance. This agent stores risk mitigation strategies in knowledge base.

4.4 Risk Mitigation Autonomic Agents Algorithm

1. Algorithms for knowledge collection Agent

```
Agent AddNewRisk (K, SIZE, F-Agent, R-Agent, RISK)
K   Agent
SIZE Knowledgebase size
F front Agent
R rear Agent; RISK information to be added at the rear of risk table.
Step1 :{ Check risk knowledgebase status}
If R-Agent>=SIZE then
  Printf ('Knowledgebase is full')
  Return
Step2 :{ Increment rear Agent}
        R-Agent=R-Agent+1
Step 3 :{ Add new risk information at rear end of Knowledgebase risk table}
        K[R-Agent] =RISK
Step 4 :{ If initially, the knowledgebase is empty, adjust the front Agent}
  If F-Agent=0, then F-Agent=1
```

2. Algorithms for analysis agent

Analysis Agent, Knowledgebase, Expert, Risk details

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

3. 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. Algorithms for evaluation agent

```
Evaluation Agent (E)
K    Knowledgebase, R Risk Mitigation results

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
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 Mitigation risk values}
  For K value E to R
        Print (K [R])
  R=R+1
```

5. Algorithms for risk monitoring agent

```
Algorithm is Monitoring agent (val Email<Risk>) system users
Step 1: Pre- Risk data is valid
Post- returns Risk status
Return- Boolean, true: risk data; false: risk available
Step 2: If (risk details available)
Email Result= true
Step 3: Else if expert user adds new risk comment
Return Send email result of risk status
Step 4: Else if staff user adds new risk comment
Return Send email result of risk status
Else
Result = true
End if
Return email result
```

6. 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
```

```
Post- risk empty and all nodes convert
Step 2: Loop (risk.front not null)
risk.front = risk.front->next
Convert (risk format)
Step 3: End conversion
Front .count = 0
Return
End conversion risk
```

7. Algorithms for report agent

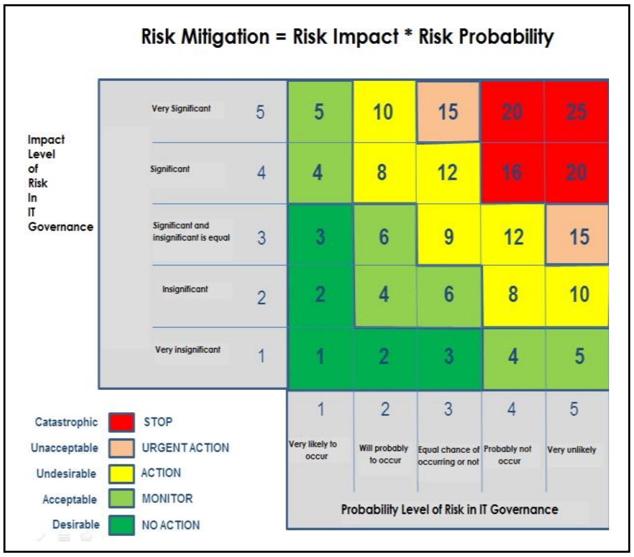
```
Agent  GenerateRiskReport (R)
R     Agent
Step1: {Check risk mitigation information values}

If Risk Data<0
      Print ('There is no Report on this risk')
Step2 :{ Display Risk information values}
   For I value F-Agent to R-Agent
            Print (R[I])
   I=I+
```

8. Algorithms for codification agent

```
Codifies Knowledge Agent (ref risk <metadata>) // initializes metadata for a risk
Pre risk status for metadata of the risk
Post metadata initialized
Step 1: Risk.add = 0
Step 2: Risk.search
Step 3: Risk.update
Step 4: Risk.delete
Step 5: Return
End Display Risk from Knowledgebase
```

4.5 Risk Measurement Autonomic Agent Technique

Table 4 and Table 5 are used by the agents to view and report the condition of the risk. This is carried out based on set of predefined colors to be applied by the agents. These functions of the agents are to be deployed in the Autonomic agent prototype system.
A view of the risk either operational or technical risk will be displayed by the report agent. This can be seen in Figure 5. The color red signifies more severe risk, orange color signifies immediate action should be taken on the risk, yellow signifies that an action should be taken on the risk, light green is just to monitor the risk situation and dark green is to ignore the risk situation.



Risk Mitigation = Risk Impact * Risk Probability

Impact Level of Risk In IT Governance		1	2	3	4	5
Very Significant	5	5	10	15	20	25
Significant	4	4	8	12	16	20
Significant and insignificant is equal	3	3	6	9	12	15
Insignificant	2	2	4	6	8	10
Very insignificant	1	1	2	3	4	5
		Very likely to occur	Will probably to occur	Equal chance of occurring or not	Probably not occur	Very unlikely

Probability Level of Risk in IT Governance

Catastrophic	🟥	STOP
Unacceptable	🟧	URGENT ACTION
Undesirable	🟨	ACTION
Acceptable	🟩	MONITOR
Desirable	🟩	NO ACTION

Figure 5 Risk mitigation impact and probability measurement

The impact/probability aims to produce a level of risk or risk rating.
Thus Risk Mitigation = Risk Impact * Risk Probability

Below is the rating scale for the risk impact and probability that is used by the measuring agent as shown in Table 4 and Table 5.

Table 4 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 5 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

5.0 RESULTS AND DISCUSSION

An agent is software that performs a specific task on behalf of a user, independently or with little guidance. Software agents are useful in automating repetitive tasks, finding and filtering information, and intelligently summarizing complex data. Autonomic computing systems are composed of groups of agents which interact with each other to achieve their goals (risk mitigation). The risk mitigation model in IT Governance has been developed using Autonomic agents. To develop the model secondary data was collected by reviewing the existing literatures on risk mitigation models. Primary data was collected by carrying out pilot study among 3 Malaysian universities using interview to collect data relating to risk mitigation to validate the data from the literatures and to test the qualitative instrument. In the pilot study 7 respondents which interviewed based on open-ended questions. The data from the pilot study was analyzed based on risk mitigation People, process, technology and quality management. After conducting the pilot study the main interview was carried out also using interview to collect data from 10 Malaysian universities comprising of 13 respondent selected using purposely sampling based on their experience, skills and knowledge on risk mitigation.

The respondents were mainly IT practitioners and IT experts. The data collected was analyzed using Nvivo Software package and was categorized and coded in risk mitigation people, technology, practice, technique, process, methods, procedures, activities, measurement and functions of a risk mitigation tool. After analyzing the data a risk mitigation model utilizing autonomic agents was developed. These agents communicate with each other by means of ACL (Agent Communication Language) messages. Here the Java language and JADE (Java Agent Development) interface which used for communication and layered is applied for architecture of agents. These agents register themselves in the Agent Platform which specifies several types of agents that can facilitate the multi-agent communication. Autonomic computing system for mitigating risk can assist risk data collection from knowledge base directly by means of database management system (DBMS) [7]. The knowledgebase consists of a number of databases that is managed by DBMS. Autonomic computing systems also use mapping techniques to produce risk mitigation knowledge.

An electronic medium, such as the Internet or Intranet, may act as an intermediary between the agents' interface and their environment by facilitating the communication and cooperation among the agents. The application of Autonomic computing systems provides the opportunity of taking advantage of the inherent capabilities of the agents. Autonomic computing systems are responsible for classifying the risky situation and predict possible risks as well as providing recommendations to manage risk situations. Autonomic computing systems can assist in mitigating risk because it has the advantage of being intuitive and capable of rather simply identifying the risk mitigation process of decision-making and how to perform it mitigation of risk based on the use of past experiences. Autonomic computing systems can help to solve risk by adapting risk solutions that have been used to solve similar problems in the past by using risk knowledgebase to retrieve, reuse, revise and retain risk data [4, 5, 7, 9, 14].

6.0 CONCLUSION

Autonomic agent technology is a rapidly developing area of research and probably the fastest growing area of information technology (IT). Autonomic agents are component of software and/or hardware which is capable of acting exactingly in order to accomplish tasks on behalf of its user. These agents are computer system situated in an environment that acts on behalf of its user. Most researchers agree that autonomy is a crucial property of an agent, thus agents autonomy precisely defines them [15]. Agent based technology has been utilized to mitigate risk in IT Governance using multi agents. However, there is still a growing need of developing innovative tools that can help IT Practitioners to solve risk in IT Governance. Existing risk mitigation approaches or tools lacks need for adequate data which is very important in mitigating risk and there is the difficult of mitigating risk generally in IT Governance. This paper presents a multi agent-based to assist IT practitioners in mitigating risk in IT Governance. These agents work collaboratively to in risk identification, risk decision, risk treatment and risk monitoring to successfully mitigate risk. These multi agents utilize data from previous risk cases to build a qualitative measuring scale to define and calculate the risk probability and risk impact.

Acknowledgement

We are grateful for the Universiti Putra Malaysia (UPM) financial support for the project.

References

[1] John, D., Isaac, N. and Admire, K. 2009. Intelligent Risk Management Tools for Software Development. *SACLA 2009 29 June-1 Mpekweni Beach Resort South Africa*. 33-40.

[2] Siridech, K., Corbitt, B. and Pittayachawan, S. 2008. ICT Risk Management in Organizations: Case studies in Thai Business. *19th Australasian Conference on Information System 3-5 Dec 2008 Christchurch*. 513-522.

[3] Mirela, G. 2011. Risk Management in IT Governance Framework. *The Bucharest Academy of Economic Studies Romania*. 14(3): 545-552.

[4] Mohammad, R. N., Koen, B. and Stamatis V. 2007. Autonomic Computing Systems: Issues and Challenges. Computer Engineering Laboratory Faculty of Electrical Engineering, Mathematics, and Computer Science Technical University of Delft, the Netherlands. 538-543.

[5] 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. doi:10.1016/j.eswa.2012.01.001. 6921-6931.

[6] Mihalis, G. and Michalis L. 2011. A Multi-agent Based Framework for Supply Chain Risk Management. *Journal of Purchasing and Supply Management.* doi:10.1016/j.pursup.2010.05.001. 23-31.

[7] Masoomeh, M., Abdollah, A. and Monireh, H. 2013. Knowledge-collector Agents: Applying Intelligent Agents in Marketing Decisions with Knowledge Management Approach. *Knowledge-Based Systems*. 181-193.

[8] Xianli, S., Min, H. and Xingwei, W. 2011. Web and Multi-agent Based Virtual Enterprise Risk Management System. *IEEE 2011 Chinese Control and Decision Conference (CCDC)*. 902-906.

[9] Khoo, Y. B., Zhou, M. and Kayis, B. 2009. An Agent-based Risk Management Tool for Concurrent Engineering Projects. *Complexity International*. 1-11.

[10] Ruan, J. and Qin, S. F. 2009. A Generic Conceptual Model for Risk Analysis in a Multi-agent Based Collaborative Design Environment. *Proceedings of the 19th CIRP Design Conference Competitive Design*. 30-31.

[11] Shikha, R. and Selvarani, R. 2012. An Efficient Method of Risk Assessment using Intelligent Agents. *Second International Conference on Advance Computing and Communication Technologies*. IEEE. 123-126.

[12] Pratim, D. and William, A. 2010. Software and Human Agents in Knowledge Codification. Knowledge Management Research and Practice. *Operational Research Society*. 45-60.

[13] Davide, A., Dulmin, R. and Mininno, V. 2012. Risk Assessment in ERP Projects. *Information Systems*. doi:10.1016/j.is.2011.10.00. 183-199.

[14] Kayis, 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.

[15] Georgakarakou, C. E. and Economides, A. A. 2006. Software Agent Technology: An Overview. Agent and Web Service Technologies in Virtual Enterprises, N. Protogeros (ed.), Idea Group Publication. 1-21.