Jurnal
Teknologi

Full Paper

MITIGATING OPERATIONAL, TECHNICAL AND STRATEGIC RISK IN ICT THROUGH KNOWLEDGE CODIFICATION TECHNIQUE

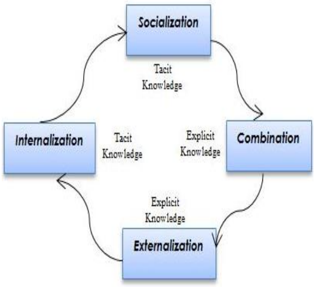
Bokolo Anthony Jnr and Noraini Che Pa*

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

*Corresponding author
norainip@upm.edu.my

Article history
Received
16 November 2015
Received in revised form
22 March 2016
Accepted
16 March 2016

Graphical abstract



Abstract

Recently, organisations have incorporated various methods into their business process in mitigating risk. Although, Information and Communication Technology (ICT) practitioners is not capable mitigate the identified risk systematically due to the high magnitude of loss caused by operational, technical and strategic risk. The ICT practitioners need to improve their ability to identify and mitigate the risks to ICT infrastructures. Besides that ICT practitioners in organization find it difficult to mitigate risks if they don't utilize completely their knowledge. There is need for ICT practitioner to codify knowledge, especially through the development of policies and practices to guide decision makers in mitigate risk in their organizations. The aim of this paper is to develop a process model for capturing, storing, disseminating and utilizing risk knowledge of knowledge-based supporting ICT practitioners to make decisions. Quantitative research methodology was adopted for reviewing of existing risk mitigation approaches in ICT and carrying out a survey using questionnaire among ICT practitioners. The questionnaire was used to validate the developed process model. Findings from the questionnaire confirms that the developed process model can assist ICT practitioners in mitigating operational, technical and strategic risk based on the codification of past knowledge of risk experts.

Keywords: Risk, operational risk, technical risk, strategic risk, risk mitigation, ICT and knowledge codification.

Abstrak

Hari ini, organisasi telah menggabungkan pelbagai kaedah dalam proses perniagaan mereka untuk mengurangkan risiko. Walaubagaimanapun, pengamal Teknologi Komunikasi Maklumat (ICT) masih belum berupaya mengurangkan risiko yang dikenal pasti secara sistematik ditunjukkan oleh magnitud kerugian yang tinggi disebabkan oleh risiko operasi, teknikal dan strategik. Oleh itu pengamal ICT perlu memperbaiki keupayaan mereka untuk mengenal pasti dan mengurangkan risiko yang berkaitan dengan infrastruktur ICT. Pengamal ICT dalam organisasi mendapati sukar mengurangkan risiko jika mereka tidak menggunakan pengetahuan mereka sepenuhnya. Terdapat keperluan untuk pengamal ICT untuk mengekodkan pengetahuan terutama melalui pembangunan polisi dan amalan untuk membimbing pembuat keputusan dalam mengurangkan risiko dalam organisasi mereka. Tujuan kertas kerja ini ialah untuk membangunkan satu model proses yang mengumpul, menyimpan, mengagih dan menggunakan pengetahuan risiko berasaskan pengetahuan untuk menyokong pengamal ICT dalam membuat keputusan. Pendekatan kajian kuantitatif telah digunakan untuk menyemak pendekatan mengurangkan risiko yang sedia ada dalam ICT dan melaksanakan satu tinjauan melalui soal selidik di kalangan pengamal ICT. Soal selidik turut digunakan untuk mengesahkan proses pembangunan model. Hasil soal selidik mengesahkan tentang proses pembangunan model dapat membantu pengamal ICT dalam mengurangkan risiko operasi, teknikal dan strategik berdasarkan pengekodan terhadap pengetahuan lepas pakar risiko.

Kata kunci: risiko operasi, risiko teknikal, risiko strategik, pengurangan risiko, ICT dan pengetahuan kodifikasi

1.0 INTRODUCTION

Risk is considered as possibility of occurrence or event or condition that will have a positive or negative effect on a project. Risk mitigation is in place to ensure that risks have been adequately resolved in the organization [1]. Risk mitigation makes it easier to cope with risk and ensure that these risks don't lead to unacceptable situation through identifying, making decision, treatment and monitoring the impact of risks. In order to minimize and control these risks successfully, ICT risk mitigation policies and strategies have been developed and implemented in organizations [2, 3]. Risk mitigation emphasizes taking action early in a project to prevent the occurrence of undesired events or to reduce the consequences of their occurrence. Risk mitigation mainly involves transferring, avoiding, controlling and accepting risk [4]. ICT practitioners have to mitigate risks (operational, technical and strategic risk) that occur when using IT infrastructures. The mitigation of these risks is necessary for proper utilization of IT infrastructures.

Knowledge Codification (KC) involves the sharing of experience, expertise, know-how, and learning from one ICT practitioner to another. Knowledge codification (KC) assists to acquire, store, retrieve and use up-to date knowledge [5]. Thus KC can support ICT practitioners in organizations by collecting, processing and using knowledge with high accuracy, speed and efficiency in mitigating risk. Knowledge codification can be used as a routine to store, extract, transform, convert and display data for ICT practitioners reuse. Thus the codification of knowledge aims to shift the ownership and control of knowledge from the experts to other practitioners in the organization.

According to [6] risk mitigation should be bases on best available knowledge. Thus knowledge codification practices use the best available knowledge within the organizational knowledgebase and help decision-makers to mitigate risk effectively. In mitigating risks in ICT, there is need to determine how existing practitioners can capture the know-how, skill and experience in risk mitigation from previous practitioners, experts or staffs in their organisation? To address this issue, there is need for ICT to adopt a knowledge retention practice that will assist to create a persistent knowledge repository to address these issues. Knowledge utilization as a key organizational resource in mitigating risk in ICT must begin with a rigorous approach toward not only creating knowledge but also systematically codifying and embedding knowledge into risk mitigation routines. Knowledge codification is more than simply cleaning information and making it usable and comprehensive. Instead, it is fragile and persistent process of scanning, interpretation, assimilation, and learning across organization [5].

ICT practitioners and decision makers indispensably rely on intuition, judgment and individual experience during risk mitigation. This is due to the lack of data needed to measure risk magnitude which usually leads to inconsistencies in risk ratings. However, the knowledge gained in mitigating risk may be codified and stored properly. Thus knowledge previously gained in mitigating risk can be reused for future risk mitigation to enhance decision making process when carrying out risk mitigation.

Thus this paper proposed a process model that codifies knowledge by using previous risk mitigation best practices as reference based on the preferences of ICT practitioners and experts. A knowledgebase has been incorporated into the process model so that new ICT practitioners and decision makers may refer to risk event histories of previous risk mitigation to make estimations on how to mitigate risk. The structure of this paper is organized as follows: section 2 presents the literature review. Section 3 describes the methodology used in this research Section 4 describes the proposed process model. Section 5 is the validation of the model based on a survey. Section 6 is the discussion section. Finally section 7 is the conclusion and future works.

2.0 LITERATURE REVIEW

Effective risk mitigation is integral to ICT well-being, thus utilization of organization's knowledge has truly become a mainstream and strategic management tool. This is simply because it's difficult for ICT practitioners to mitigate technical, operational and strategic risk effectively, if they cannot manage their knowledge. Thus this section explains on risks in ICT, overview of knowledge codification practice in relation to risk mitigation carried out by practitioners in ICT.

2.1 Risks in ICT

Practitioners are faced by technical, operational and strategic risk occurs in ICT.

a. Technical risk

Technical risk considers factors such as processing capacity, access control, data protection, and cyber-crime. Technical risk also relies on expected functions and behaviours of installation components. Technical risk is the most important risk which comprises of technology system failure. Technical risk is mostly associated with emerging technological issues. Technological problems can arise from application of a new process, material, or subsystem due to misunderstanding the parameters that control performance, cost, safe operating latitudes, or failure modes. Technical risk can disrupt all activities in organisations. Technical risk is highly dependent upon a correct and detailed understanding of the specific technical requirements [7].

Technical risk can occur if a previously commercialized technology is extended outside the known domains of the pertinent design rules or from unexpected interactions arising from a new or unique combination of subsystems or components. Technical risk does not exist in isolation in ICT, but rather it's highly influenced by practitioner's capability and experience to understand and deal with changes in ICT.

b. Operational risk

Operational risk is the risk of direct or indirect loss resulting from inadequate or failed internal processes, people, systems and external events. Operational risk includes anything that can have impact on the overall performance of ICT ability to create value, which includes events such as mistakes or missed opportunities [8]. Operational risk may arise due to internal events such as the potential for failures or inadequacies in any ICT processes and systems, or those of its outsourced service providers. Operational risk that arising from human resources may refer to a range of issues such as mismanaged or poorly trained employees, the potential of employees for negligence, wrongful misconduct, conflict of interest, fraud and rogue trading. Therefore the emergence of mistrust, failure to communicate, low morale and cynicism among staff members, as well as increased turnover of staff, should be regarded as indicative for potential increase in operational risk [9].

There are four main causes of operational risk that are identified in standard operational risk definitions. Operational risk is due to issues arising from people (human factors), processes, systems, and external events. A successful operational risk program combines qualitative and quantitative approaches to ensure operational risk is both appropriately measured and effectively managed. Operational risk assessment mostly cover risk's appetite and tolerance for operational risk, as specified through the policies for managing this risk, including the policies that outlines ICT firms.

c. Strategic risk

Strategic risk relates to risk at the corporate level, and it affects the development and implementation of ICT strategy. In developing a strategy, ICT practitioners usually make an assessment of IT infrastructures condition and forecast based on changes that will occur over a period of time. Strategic risk includes risk relating to the long-term performance of ICT [10]. Strategic risks also tend to be more complex and difficult to assess than operational risk.

Strategic risk mitigation is a process for identifying, assessing and controlling risks and uncertainties, affected by internal and external events or scenarios. Strategic risk inhibits ICT ability to achieve its strategy and objectives with the ultimate goal of creating and protecting shareholder, stakeholder value, IT infrastructure usage and policies [11]. Strategic risk involves the evaluation of risks relating to the organization's mission and strategic objectives, typically performed by senior management teams in strategic planning meetings, with varying degrees of formality. Strategic risk includes risk relating to the long-term performance of the organization. Strategic risks are identified by practitioners by implementing a continual process that is embedded in strategy setting, strategy execution, and strategy management [10].

2.2 Importance of knowledge in risk mitigation

Knowledge is the collection of know-how, expertise, experiences, and instincts that assist in the interpreting and understanding of information. Knowledge has been conceptualized as actionable information, thus more effectively assisting in the decision-making processes within the organization. Knowledge is mainly the combination experience, values, contextual information, and expert insight. Knowledge often becomes embedded, not only in documents or repositories, which are easily shared among organizations, but also in ICT routines, processes, practices, and norms [3]. Risk mitigation serves as a supportive mechanism for practitioners' in making decisions on ICT usage to accomplish business objectives and continuity. More recently, ICT practitioners have incorporated knowledge management methods and practices into their business processes. Existing ICT tools and techniques attempt to codify tacit knowledge into formal systems. However, this generates issues since the informal and locally situated practices that allow ICT practitioners to mitigate risk, is not easy to implement. In the context of developing an approach for mitigating technical, operational and strategic risk that surface in ICT, practitioners may codify risk knowledge by capturing, storing and distribution of knowledge, especially through the development of explicit policies and practices to guide decision makers and other practitioners. Nevertheless the ability to codify knowledge is linked to the social practices of creating and sharing knowledge [12]. According to [4] knowledge relevant and important to organization knowledge to be made explicit using active knowledge tools, effective technology, and human resource management, to ensure that it is continuously transferred via organizational repository. Technical, operational and strategic risk knowledge is needed to mitigate the risk in ICT. While operational and technical risk knowledge is concerned with the day-to-day running of the business, strategic risk knowledge is essential to major decisions an organization must make to capitalize on priority opportunities and successfully overcome risks [4].

2.3 Dimension of Knowledge

Knowledge may be divided into two forms: explicit and tacit. Explicit knowledge is formal and systematic. It is therefore easily communicated and shared throughout the firm. For example, explicit knowledge is embodied in a computer programme or set of procedures for hiring staff. ICT firms establish many examples of explicit knowledge, indicated by their complex administrative procedures and controls. There is considerable debate by academicians and researchers regarding various types and dimensions of knowledge. In particular, the distinction between tacit and explicit knowledge receives substantial attention. Tacit knowledge is defined as highly personal and not amenable to formalization and standardization. In addition, tacit knowledge is not easily communicated across organization. [13] mention that tacit knowledge is deeply rooted in action and in individual's commitment to a specific context, which is usually a craft or profession, related to a particular technology or product market, or the activities of a work group or team. Tacit knowledge consists partly of technical skills, the kind of informal, hard to pin down skills captured in the term know-how [13]. [13] went further to say that the knowledge creating firms should attempt to make tacit knowledge explicit by codifying the knowledge. In summary Tacit knowledge is knowledge held in the minds of individuals, while explicit knowledge is that externalized and shared with others. It has been suggested that there are four modes of interaction between these two forms of knowledge (tacit and explicit Knowledge):

a. From tacit knowledge to tacit knowledge: the process of *socialization* through shared experience and interaction;
b. From explicit knowledge to explicit knowledge: the process of *combination* through reconfiguring existing knowledge (such as sorting, adding, recategorizing, and reconceptualising explicit knowledge) can lead to new knowledge;
c. From tacit knowledge to explicit knowledge: the process of *externalization* using metaphors and figurative language; and
d. From explicit knowledge to tacit knowledge: the process of *internalization* through the learning process [4].

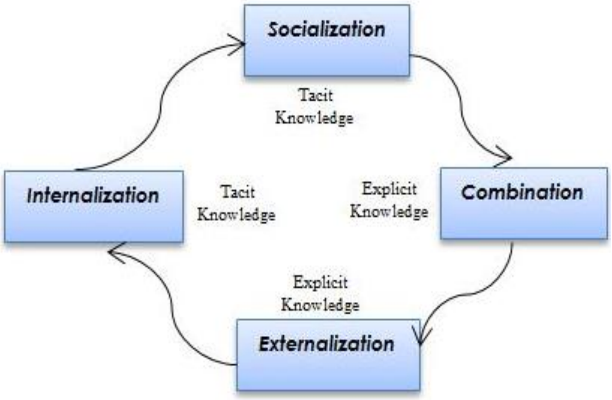


Figure 1: Spiral of Knowledge Creation [13].

Figure 1 shows the creation of knowledge, as seen from tacit to tacit knowledge produces *socialization*. Observation and practice are two knowledge capture tools explicit to explicit knowledge *externalizing* via analogies or metaphors. Resulting explicit knowledge can then be stored in repositories. Next is explicit to tacit knowledge *internalizing* explicit knowledge into tacit knowledge. Lastly tacit to explicit knowledge *combining* or sorting different knowledge to lead to new knowledge. Hence the key to a proactive risk mitigation process lies in the firm's ability to mobilize the knowledge and expertise of its practitioners so that other ICT practitioners can ensure that they get accurate and timely information about a potentially risk. In fact, many experts agree that ICT practitioners can't mitigate risk today without utilizing its knowledge [14].

2.4 Overview of knowledge codification

Knowledge Codification (KC) is the representation of knowledge such that it can be accessed and transferred as explicit or tactic knowledge. It converts tactic knowledge into explicit usable form by converting undocumented information into documented information, representing and organizing knowledge before it is accessed. Knowledge codification also involves converting "tacit knowledge" into explicit usable form. KC involves converting undocumented information into documented information. Representing and organizing knowledge before it is accessed. It makes institutional knowledge visible, accessible, and usable for decision making. KC is important to ICT practitioners in mitigating risk in so many ways such as;

a. Instruction/training—promoting training of ICT practitioners based on captured knowledge of senior practitioners on how to mitigate risk in ICT.
b. Prediction—inferring the likely outcome of a given risky situation and reporting a proper warning or suggestion for risk mitigation action.
c. Diagnosis—addressing identifiable risk and mapping out the specific causal cause of the risk.
d. Planning/scheduling—mapping out an entire mitigation of action before any steps are taken.

Thus KC allows the modularization of knowledge, which facilitates specialization and allows firms to acquire knowledge at a fixed cost, which in turn facilitates the outsourcing of activities. KC directly affects knowledge creation, innovation and economic growth, which has the potential to alter the rate and direction of knowledge generation and distribution dramatically [15].

2.5 knowledge acquisition methods for risk mitigation

Making knowledge available to practitioners during risk mitigation is critical to decision-making process. However decision making in risk mitigation process should involve consultation with risk mitigation team members, made up of experts from a community of practice or a knowledge network, who are able to analyze, debate, and help suggest mitigation action on identified risk. The decision-making process, therefore, becomes much better informed and balanced, with contributions from practitioners who understand the situation, based on their experience with similar happenings. Thus knowledge can be codified from various mediums stated below;

a. Knowledge warehouse

The knowledge warehouse is collation of information captured from ICT know-how, lessons learnt, in-depth internal expertise, case studies, internal and external case-based knowledge, best practices external benchmarking and engineering standards. The access to such knowledge means that the risk repository is capable of enabling the use of past successes and failures captured to mitigate risks in ICT. Thus, knowledge warehouse is a useful tool for informing practitioners on several aspects of mitigating operational, technical and strategic risk in ICT.

b. Case studies

Case studies based on specific ICT projects were primarily used either through interviewing or capturing information and identifying critical success and failure factors. A database of risk items 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 measurement. All these constitute the database of case studies.

c. Lesson learnt

The knowledge elicitation of lessons learnt is the extension of case-based studies which capture in-house past experiences in more detail. The success of any ICT project can be enhanced by considering successes and failures of previously completed ICT projects. 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. Additionally, it also captured information from different aspects of any project depending on their specific role in the team, background, experience and personality.

d. Best practices

Benchmarking of other successful organisations is a technique often used by ICT experts to strive for excellence. Various best practice web sites are used to gather information with respect to successful risk mitigation, readily available from an array of ICT firms. Hence, the application of best practices by ICT practitioners not only provides an avenue for transferring excellence from several sources into the organisations, but also serves to populate the database with respect to identification of risk items and mitigation strategies.

e. Knowledge mapping

Knowledge mapping is a process by which ICT firms determines who knows what in the organization. It has many forms, including skills mapping, where employees list specialty knowledge and project experience, which is then codified in a relational database and made available through the firm's practitioners. Sometimes known as "knowledge yellow pages" This skills and experience mapping allows a company to understand where experience and expertise lies in the company, and where needed skills or knowledge may be missing.

f. Community of practice

Communities of practice are naturally-forming networks of employees with similar interests or experience, or with complementary skills, who would normally gather to discuss common issues (such as mitigating risk in ICT). Presently, communities of practice are actively identified, and members of these networks are encouraged to gather and exchange ideas concerning potential risk activities on a formal basis, capturing lessons learned, swapping ideas, and sharing insight.

g. Hard Tagging

Hard tagging is a knowledge management process that combines knowledge mapping with a formal mentoring process. As part of the knowledge mapping and skills mapping process, experienced practitioners are identified or "hard tagged" so they will become part of a consultation pool that will be available when special advice is needed on developing issues. These hard tagged specialists also team in communities of practice with "soft tagged" practitioners those who are interested in learning specialist skills or in sharing experience in a mentoring and knowledge sharing exercise.

h. Learning

One of the most important principles of knowledge is that practitioners should share experiences and techniques with others in the firm, so that there is a continuous and dynamic process of knowledge sharing and learning taking place. One of the greatest benefits from this process of continuous learning is that practitioners emulate lessons learned from previous risk mitigation in their firms.

2.5 Existing knowledge approaches toward managing risk

Researchers have attempted to incorporate knowledge techniques in risk management, using various techniques. [16] developed a reference model for organisations and project management which codifies knowledge in terms of fuzzy set theory. The proposed approach therefore allows for the codification of explicit and tacit knowledge and a new model is presented which integrates both explicit and tacit knowledge as measures within the project risk assessment base from the experts. The proposed approach of risk assessment is also used as a decision support thus used by the professionals to quantify risk ratings. The model provide guidance for company about risk based on past, using rule base that can be verified according to past experiences with risk assessment, thus for organizational learning. [17] Reviewed the ISO 9000 standards relating to the codification process in two ways. First, to codify knowledge the ISO 9000 standards used as a codification tool, which allows a firm to formalize the codified knowledge within the firm. [14] researched on managing corporate risk through better knowledge management; in his research he developed a corporate integrity framework, and then explores how the process component of the framework uses knowledge management related procedures, techniques, and tools corporations. The researcher maintained that KM procedures, techniques and tools are being used to perform risk management via the integration of knowledge and risk management.

[18] Analyze the integration of Knowledge management techniques into the activity of risk management as it applies to software development projects. The researchers argued that knowledge is essential to carry out activities in these ICT; however, much of this knowledge is still in the realm of tacit knowledge (experience), embedded initial efforts for the purpose of storing this knowledge for use in risk management.

[6] Proposes a knowledge-based risk mapping approach for systematically assessing risk-related variables that may lead to cost overrun. Their approach is based on previous projects of partner firm as test cases and preferences of ICT professionals. Their approaches also make use of practitioners about level of risk and magnitude of potential risk events, lessons learned database was incorporated into the tool so that decision-makers may refer to risk event histories of previous projects to make estimations about forthcoming projects.

[12] Developed a knowledge-based risk assessment framework which incorporates key performance indicators (KPIs) for evaluating the benefits and risks of web-enabled application outsourcing projects. The framework aims to introduce rigor into how customers evaluate consortium, project-based application outsourcing. [4] designed a tentative knowledge process model for strategic risk approach to knowledge management. The researcher mentioned the relevance and importance of knowledge in an organization. The researcher encourages organisations to codify their knowledge using knowledge management approaches, to ensure that knowledge is continuously transferred via the organizational memory or repository.

[19] Develop a model for risk management of knowledge risk in a project-based organization. The integrated KM and RM model can be used to assist the planning, establishment and evaluation of knowledge risk in projects. [20] published their research on how knowledge management processes can improve the implementation of Enterprise Risk Management (ERM). Their aims is to understand the value of people interaction and technological support in an ERM program that implies multiple disciplines, profiles, groups of people with different knowledge and experiences working together.

3.0 RESEARCH METHODOLOGY

In this paper, a review research approach was adopted, which involves the examination of existing practices to develop a model based on the literature review and considering the strengths and weaknesses observed in past studies, the authors decided to firstly review knowledge codification concept in relation to risk mitigation. This will serve as a basis for developing a new process model that codifies knowledge for risk mitigation for ICT practitioners. Next the proposed process model is developed; lastly the process model is validated based on a survey using a questionnaire.

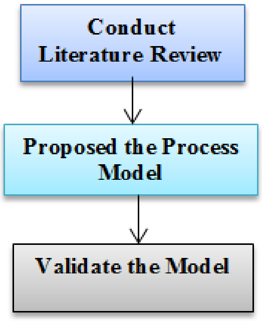


Figure 2: Research Methodology for this paper

Figure 2 shows the methodology used for this research to propose the process model for mitigating risk in ICT using Knowledge codification practice. As stated above this research started with the review of risks that occurs in ICT (operational, technical and strategic risk). Next is the review of existing literatures on knowledge codification in general and in relation to risk mitigation approaches. The last phase is the study on risk mitigation.

3.1 Theoretical framing of knowledge codification and risk mitigation

This section presents the main concepts regarding knowledge codification and risk mitigation.

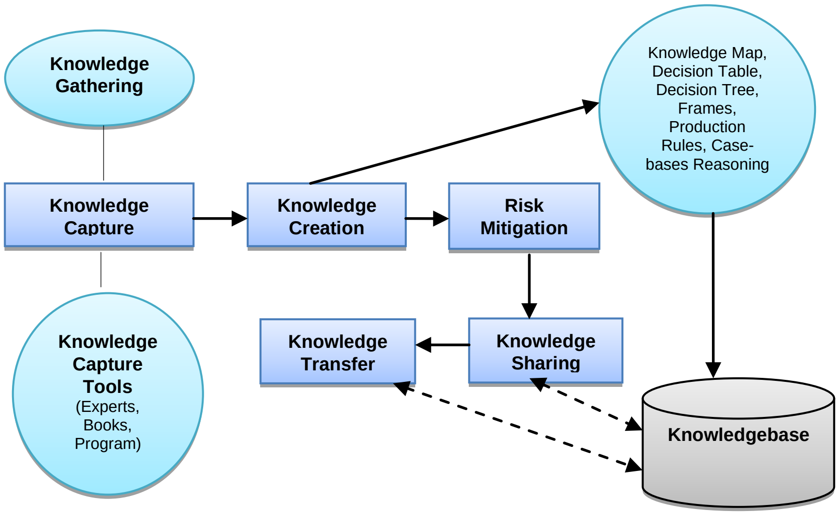

Knowledge Gathering
Knowledge Capture
Knowledge Creation
Risk Mitigation
Knowledge Map, Decision Table, Decision Tree, Frames, Production Rules, Case-bases Reasoning
Knowledge Capture Tools (Experts, Books, Program)
Knowledge Transfer
Knowledge Sharing
Knowledgebase

Figure 3 Knowledge Codification in risk mitigation

Figure 3 shows the knowledge codification process in mitigating risk in ICT. Knowledge codification involves the transformation of knowledge into information, thus codification is a process of creation of messages, expressing pre-existing knowledge, which can then be processed as information [20]. KC aids knowledge transfer, acquisition and storage at low costs. Once knowledge is transformed into information, Knowledge is easier to codify and codified knowledge is easier to diffuse by practitioners in ICT for risk mitigation.

Knowledge codification takes place when knowledge is written down in books and manuals, stored on films (e.g., instructional videos) or embedded in everyday work procedures or software (e.g., diagnosis software, expert systems).
These media are widely used and serve the purpose of articulating, transferring and storing explicit human knowledge. Therefore knowledge codification is the process by which explicit knowledge is detached from its source and put in a state in which it can easily be transferred via different media, such as software or books. Different types of codification can be differentiated: knowledge can be embedded in machines or software (e.g., robots, workflow software) or codified in detailed process descriptions and manuals that prescribe how knowledge should be used.

Knowledge codification and risk mitigation are based on the interactions among people, which correspond to the movements from tacit and explicit knowledge to tacit and explicit knowledge on the individual and organizational level) [20]. In risk mitigation this interaction is expressed through socialization, combination, externalization and internalization (see section 2.3). Socialization is the social interaction among the risk management employees and shared risk modeling experience. Combination is the merging, categorizing, reclassifying and synthesizing the risk modeling process. Externalization is the articulation of best practices and lessons learned in the risk modeling process and Internalization involves learning and understanding from discussions and mathematical modeling review [20]. In relation to risk mitigation, knowledge codification plays an important role as potential enablers of working skills and to improve the capacity of ICT practitioners to enhance the medium that they share knowledge and the tools that they use.

Table 1 Knowledge Codification in risk mitigation

Modules	**Description**
Knowledge Gathering	In risk mitigation new risk implies new ways to measure and identify potential. Knowledge gathering involves ways of understanding new and current risks.
Knowledge Creation	Involves the collection of risk knowledge from various knowledge sources in the organisation. It involves the creation of knowledgebase.
Knowledge Capture	This is the phase where the risk knowledge is produced. The tacit knowledge is collected from the experts in the organization.
Knowledge Transfer	This phase involves the dissemination and distribution of knowledge in order to support practitioners to develop risk mitigation strategies.
Knowledge Sharing	This phase is the utilization of the codified tacit knowledge as explicit knowledge by practitioners in ICT to mitigate risk.
Knowledge base	Saves risk mitigation strategies, by organizing and representing of risk knowledge. This includes the activities of preserving and maintaining of risk knowledge.
Knowledge	The classification process is the conversion

Classification	of knowledge into categories that can be processed as information. Classified knowledge can be characterized as information-like and objectified. Knowledge codification is carried out by tools as seen in Section 3.2 of this research paper.
Knowledge capture Tools	Involves the knowledge gotten from the experts in the organisations based on their past experience and their skills in mitigation risk. Other tools are the books (user manuals) and other programs that assist in mitigating risks in ICT.

3.2 Knowledge codification tools

This section explains briefly existing knowledge codification tools;

a. Knowledge map

It's a visual representation of knowledge, not a repository. Identify strengths to exploit and missing knowledge gaps to fill. Knowledge map can be applied in knowledge capture. Thus it is a straightforward directory that points practitioners to where they can find certain expertise. It captures both explicit and tacit knowledge in documents.

b. Decision table

It's more like a spreadsheet divided into a list of conditions and their respective values and a list of conclusions. Conditions are matched against conclusions.

c. Decision tree

It is a hierarchically arranged semantic network. Composed of nodes representing goals and links representing decisions or outcomes. Read from left to right, with the root being on the left. All nodes except the root node are instances of the primary goal. It is based on the ability to verify logic graphically in problems involving complex situations that result in a limited number of actions.

d. Frames

It represents knowledge about a particular idea in one place. It helps to handle a combination of declarative and operational knowledge, which make it easier to understand the problem domain. Frames usually possess a slot (a specific object or an attribute of an entity) and a facet (the value of an object or a slot). When all the slots are filled with values, the frame is considered instantiated.

e. Production Rules

It's a form of tacit knowledge codification in the form of premise-action pairs. It uses rules based on conditional statement that specify an action to be taken if a certain condition is true. The form is IF… THEN, or IF…THEN…ELSE. A Boolean expression that must be evaluated as true for the rule to be applied Action: Second component, separated from the premise by THEN; executed if the premise is true.

f. Case based reason

Case bases reasoning (CBR) is knowledge from relevant past cases in a manner similar to humans' use of past experiences to arrive at conclusions. Goal is to bring up the most similar historical cases that match the current case. CBR has more time savings than rule-based systems. It usually requires rigorous initial planning of all possible variables. Thus case based reasoning is applied by the proposed process model as seen in Section 4.0.

4.0 PROPOSED PROCESS MODEL

Below is the proposed risk mitigation process model. The model is developed based on knowledge codification (Using Case based reasoning). Figure 4 shows the risk mitigation process model. The proposed process model aims to provide timely and contextual knowledge to decision makers and practitioners. The model supports decision making in knowledge-intensive environments such in ICT.

The process model utilizes the codification of knowledge that aims at reducing and converting knowledge into messages. These messages can then be processed as information that will serve to re-form knowledge at a later time, in a different place, or by different practitioners in ICT. The transformation of knowledge in the model is to facilitate the treatment of knowledge as an enterprise good, which can be used for mitigating risk in ICT. Therefor the process model comprises of an enterprise knowledgebase which captures and stores lessons learned from previous projects and enables learning from previous projects to support decision making in forth coming projects is needed. The enterprise knowledgebase contains experts' lessons learned by conducting several face-to face interviews and review sessions with risk mitigation experts. Real risk event histories of previous projects (that are called as project cases) are captured by interviews and risk-related information are also stored in the enterprise knowledgebase.

Moreover, the performance of the process model significantly depends on the knowledge sources of the firm and the quality of the lessons learned in the enterprise knowledgebase. To improve the quality of risk mitigation strategies as defined by the experts the enterprise knowledgebase should be seen as an initial platform which can be improved by company feedback and its performance can be enhanced by increasing its intelligence by increased knowledge sources fed into it.

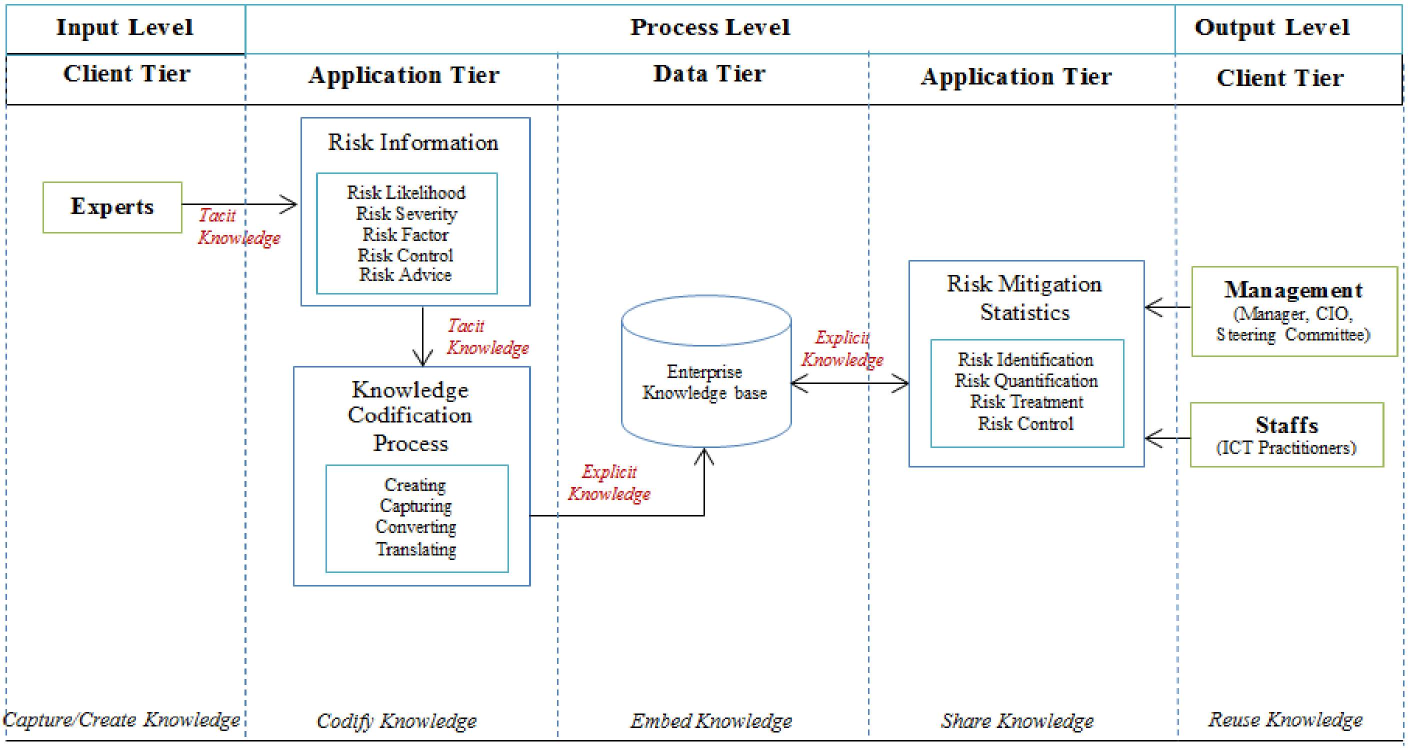


Figure 4 Risk mitigation process model based on knowledge codification technique (CBR)

Figure 4 shows the proposed process model that codifies knowledge to mitigate operational, technical and operational risk in ICT.

4.1 Model levels

The model levels are;

a. Input level

The input layer is responsible for collecting data on operational, technical and strategic risk from web, documents, profiles, tacit knowledge of experts that is collected by software like workgroup software. Then it filters, synthesizes and extracts knowledge from this information by using different approaches such as knowledge mapping. Finally, the layer checks the knowledge base whether it contains the same as new knowledge. If it does not find the same new knowledge in knowledge base, it accepts new knowledge and sends it to the process layer.

b. Process level

This layer is responsible for locating and retrieving related risk knowledge and disseminates new knowledge that may be of interest to certain groups, as well sharing the knowledge among practitioners. This layer also recommends an appropriate mitigation strategic by assisting practitioners to mitigate risk via the enterprise knowledgebase, view their solution, give feed backs about risk solution, access new interested Knowledge, save their knowledge and behavior, and view recommended decisions to the firm. In this layer the knowledge, which is useful for risk mitigation is stored in knowledge base.

c. Output level

This layer is responsible for retrieving risk knowledge that may be of interest to practitioners. This layer first looks at practitioners profile to find the interests of user and it also looks at knowledge map to find user's expert then connects to knowledge base. Then it retrieves risk knowledge that may be of interest and are related to his/her expert. Finally this layer sends the addresses of statistical results to user interface to be shown. This layer also updates and edits the knowledge by removing the outdated knowledge and collecting the feedbacks of practitioners and decision maker about the application of knowledge in their decisions to mitigate risk.

4.2 Model tiers

The model process tiers are;

A. Client tier

The client tier is the interface of the experts, management and staffs in the firm. The client tier is used to send command and receive statistical reports from the knowledge. The experts use the client tier to codify tacit knowledge, while the management and staffs use the client tier to utilize explicit codified knowledge to mitigate risk in ICT.

a. Expert

This are the practitioners in ICT firm that possess the skills and experience on risk mitigation based on past experience. The experts' knowledge is created and codified by transferring the locus of control and ownership of knowledge from the practitioners to other practitioners in the firm.

b. Practitioners (management and staffs)

These are the beneficiaries of tacit knowledge from the experts. The management and staff in the organisation utilize the explicit knowledge to mitigate risk ICT. The statistical report is used for making decisions on how to mitigate operational, technical and strategic risks.

B. Application tier

This is mainly the logical control tier used by the implemented programming language to collect tacit knowledge from the experts and interpret explicit knowledge to the practitioners in the firm.

a. Risk information

The risk information is the data on how to identify and mitigate risk. The risk information comprises of the risk livelihood, risk severity, risk factor, risk control and lastly the risk advice. The experts add his or her tacit knowledge on risk and the information is codified as explicit knowledge to other practitioners in the firm. Thus explicit knowledge aids the creation of tacit knowledge; tacit knowledge, when codified, adds to explicit knowledge. It is a cycle of continuity.

b. Knowledge codification process

The codification allows the building of the enterprise knowledge base that becomes the central knowledge repository under the organizational policy. In order to move tacit knowledge from the source to the seeker, firms need to codify it into explicit knowledge. As a result practitioners must rely on skills related to creating, capturing, and translating to facilitate knowledge transfers and promote codification. Codification process allows creation of a context conducive to the sharing rather than hoarding of knowledge. Thus capturing, converting and translating allows accurately understanding and interpreting across functional boundaries without losing knowledge.

c. Risk Mitigation Statistics

This phase consists of the explicit risk knowledge that has been codified and retrieved from the enterprise knowledgebase. The risk statistics contains risk mitigation strategy, which explains how to identify the risk, the risk quantification, how to treat and control the identified risk. This statistical report is used by the practitioners in the firm.

C. Data Tier

The data tier comprises of the enterprise knowledgebase that is used by the experts to add his/her tacit knowledge to be codified. The practitioners use the knowledgebase to retrieve explicit knowledge from the knowledgebase.

a. Enterprise Knowledgebase

An enterprise knowledge base serves as the organizational repository to be used for future queries employing procedural and rule-based reasoning schemes. Hence, the risk information from the experts is strategically shifted from the individuals to the organization. The knowledge base thereafter serves as source of explicit knowledge that aids knowledge discovery efforts in the future to mitigate operational, technical and strategic risk.

4.3 Tacit and Explicit knowledge codification

Tacit and explicit Knowledge process relates to how data, information, and knowledge are extracted, transformed and loaded to build enterprise knowledge bases. The phases include;

a. Capture/create knowledge

Mitigating risk implies new ways to measure it and to identify the potential effects that it could have. Knowledge acquisition, synthesis, fusion and adaptation of existing risk knowledge are parts of the way to capture and collect data on how to mitigate new and current risks.

b. Codify Knowledge

This involves the transformation of tacit knowledge into explicit knowledge in order to facilitate flows of organizational knowledge.

c. Embed Knowledge

Risk mitigation strategies, actions and methods require are codified, organized and represented as risk knowledge in the enterprise knowledgebase. This includes the activities of preserve, maintain and index risk knowledge.

d. Share Knowledge

Involves the dissemination and distribution of explicit knowledge in order to support practitioners in mitigating risk in ICT.

e. Reuse Knowledge

Risk mitigation knowledge after being codified is used as best practices and guides as standards or guidelines for risk mitigation.

5.0 MODEL VALIDATION

Survey using questionnaire was used to validate the process model. The respondents answered the questions in the questionnaire after the model was shown to them on how to carry out risk mitigation using the model. The model was evaluated based on the respondents' experiences in mitigating risk in their organisations. The developed risk mitigation process model was shown to the respondents after which the respondents were asked some questions based on the model ability to support decisions making in mitigating risk. The results from the evaluation session are shown in table 2.

Table 2 Summary of the questionnaire results

	R1	R2	R3	R4	R5	R6	Mean
Q1	5	5	5	4	5	5	4.83
Q2	5	5	5	5	5	5	5
Q3	5	5	4	5	5	5	4.83
Q4	5	5	5	5	5	4	4.83
Q5	4	5	4	4	5	4	4.33
Q6a	5	5	5	5	4	4	4.67
Q6b	5	5	5	5	4	5	4.83
Q6c	5	4	5	5	5	5	4.83
Q6d	5	5	5	5	5	5	5
Q7a	5	4	5	5	5	5	4.83
Q7b	5	5	5	5	5	5	5
Q7c	5	5	5	5	5	5	5
Q8	4	4	5	5	4	5	4.5
Q9a	5	5	4	5	5	5	4.83
Q9b	4	4	5	4	5	4	4.33
Q9c	4	4	4	5	5	5	4.5
Q10	5	4	5	5	5	5	4.83
Q11	5	4	5	5	5	4	4.67
Q12	5	5	5	5	4	4	4.67

R1-R6 is the six different Malaysian organisations that were involved in evaluating the model. Several respondents were involved in the survey from the six organisations, where Table 2 shows the results from the model session. From Table 2 Mean is the average result of each of the question.

Q1- Q12 is the questionnaire questions as seen in table 2. Microsoft excel was used to analyze the data.

5.1 Result of Usability of the Model in Mitigating Risk

In terms of the usability of the model in mitigating risk, the model is tested based on the first (1) to the fifth (5) questions which is shown in the vertical axis of the chart in Figure 5. Where R1-R6 is the cumulative response form the 6 different organisations as seen in horizontal axis of the chart in figure 5.

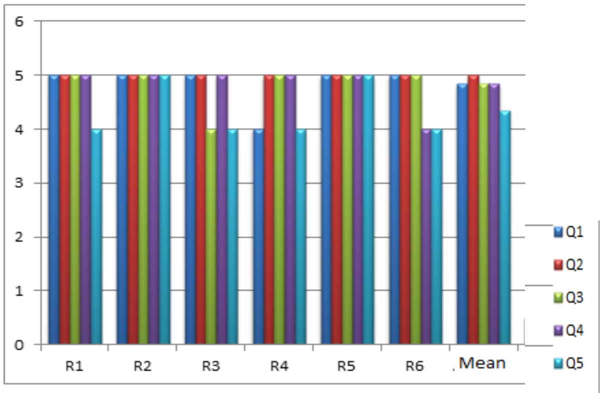


Figure 5 Result of Question 1-5

From the Q1 is the model user friendly, understandable enough? The experts' mean is 4.83 which signify that the model is completely friendly and the respondents' answers are close. From Q2 in terms of help and support provide by the model? The respondents' mean is 5 which show that the model help and support are enough for the practitioners. From Q3 is it easy to move around the model?

The respondents' mean is 4.83 which show that practitioners can easily move around with the model as seen in figure 5. From Q4 was it easy to learn how to use the model? The experts' mean is 4.83 showing that it is easy for practitioners to learn and use and diffuse the model. From the Q5 did they encounter problems in using the model? The respondents' mean is 4.33 showing that there was either less problem or no problems for in using the model.

5.2 Result of Validity of the Process Model

In terms of the validity of the process model, the model is tested based on the sixth (6) to the twelve (12) questions in the questionnaire.

From Q6 regarding the risk mitigation steps is the model sufficient to cover the risk mitigation process.

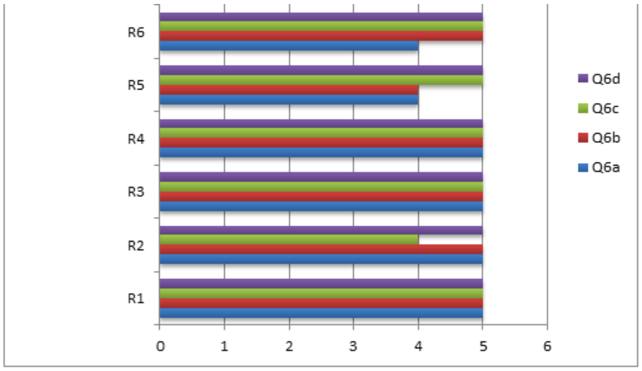


Figure 6 Result of Question 6 (6a-6d)

Where 6a is on risk identification, 6b is on risk decision, 6c is on risk treatment and 6d is on risk monitoring. The respondents' mean is 4.67 for risk identification, 4.83 for risk decision and risk treatment and 5 for risk treatment which means that the model can sufficiently cover all the risk mitigation process involved in mitigating risk in ICT as seen in Figure 6. Thus the respondents were completely satisfied with the model in respect to carrying out the risk mitigation process.

From Q7. In terms of the importance of the model carrying out risk measurement and risk statistics.

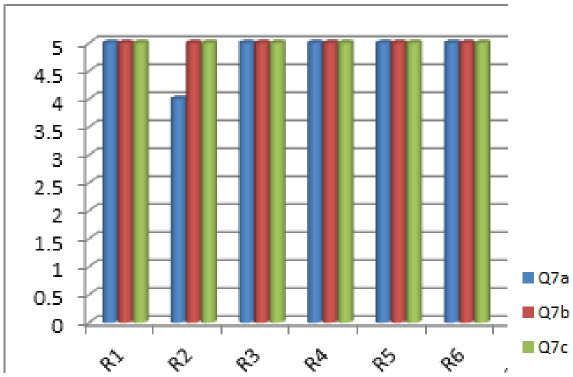


Figure 7 Result of Question 7 (7a-7c)

The respondent agreed that risk measurement is very important in the model with a mean of 4.83 as seen in Figure 7. Thus the respondents also agreed that risk statistics is very important for monitoring based on a mean of 5. The respondent agreed that risk report is very important in the model with a mean of 5.

For Q8. How efficient do the respondents think the model would be in the real use?

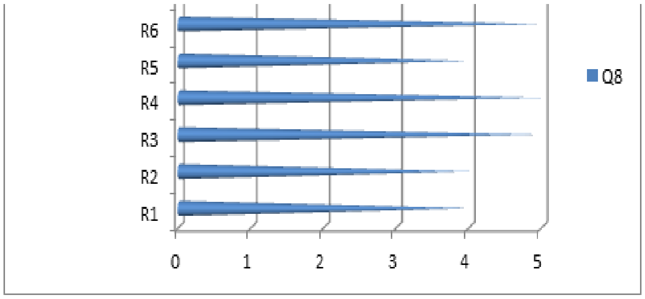


Figure 8 Result of Question 8.

The respondent agreed that the model would be *Very efficient* in the real use with a mean of 4.5 f 0.52 as seen in figure 8.

From Q9. How satisfied are the respondents with the model in terms of the models' overall performance, response time and reliability.

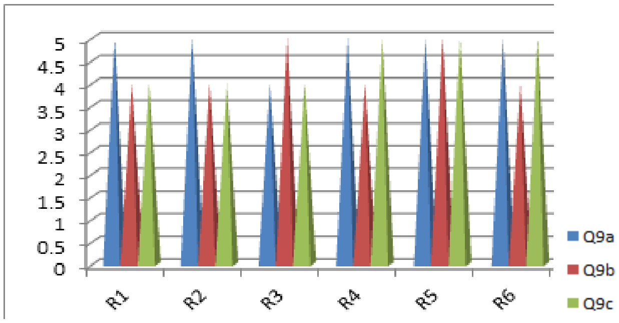


Figure 9 Result of Question 9

The respondent agreed that they are satisfied with the performance, models' response time and reliability with a mean of 4.83 for the models' performance, 4.33 for the system response time, and 4.5 for the reliability as seen in figure 9.

For Q10. In terms of how do the respondents trust and have confident in the model?

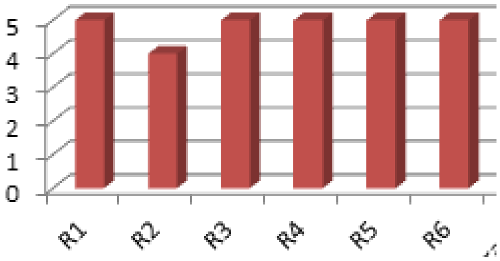


Figure 10 Result of Question 10

The respondent agreed that they have trust and confidence in the model with a mean of 4.83, in terms of accuracy of trust that the system can provide as seen in Figure 10.

For Q11. In terms of the accuracy of the model's results?

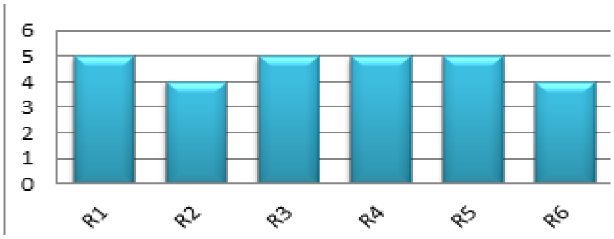


Figure 11 Result of Question 11

The respondent agreed that the results from the model are mostly accurate with a mean of 4.67, thus there is accuracy in the results from the model as seen in Figure 11.

For Q12. What is the degree of the model acceptance to the respondents?

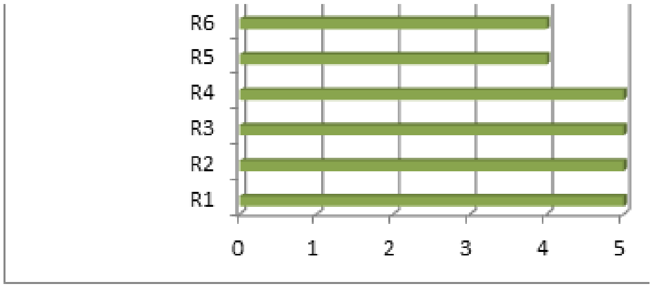


Figure 12: Result of Question 12

It can be seen from figure 12 that the model was accepted by the respondents with a mean of 4.67. Thus the model was accepted by the respondents.

6.0 DISCUSSION

Knowledge codification can be defined as the conversion of tacit knowledge into explicit one patents, databases, procedure manuals, etc. that can be processed as information. Codified rules as contained in manuals and procedures can also merely serve to provide guidelines for repetitive actions. In such instances, codification primarily serves the purpose of facilitating routine replication. The organizational benefits of codification in mitigating risk lie primarily in the re-use and diffusion of codified knowledge. Knowledge codification means converting tacit knowledge to explicit knowledge in a usable form for the organizational members. The converted explicit knowledge is organized, categorized, indexed and accessed by the network community.

Codification aims to structure and eventually build the knowledge base as knowledge repository. Based on the above theory, a system can be developed to convert the personal knowledge to explicit knowledge and store in a repository, from where the knowledge is made shared and captured in the network. Through the creation of an enterprise knowledgebase for practitioners, codification make organisations less vulnerable to loss of tacit knowledge stored ine experts. Knowledge codification facilitates the transfer of knowledge and, thus, contributes to the firm's combinative know-how in mitigating risk. In line with this, knowledge codification is important because of the gains that can be made through new combinations of stocks of codified knowledge. Typically, knowledge that is tacit resides in people, institutions or routines. Thus codification of knowledge can reduce the costs of knowledge acquisition by those who are interested in the knowledge that has been codified. Therefore, codification refers to the process of knowledge being transformed into information, where information is in the form of messages, or sets of identifiable rules and relationships, that can be transmitted to practitioners for decision making.

Evaluation of the model shows that the process model tool supports the risk mitigation decision making, thus assisting practitioners in decision making relating to risk mitigation in ICT organisation. The process model seems to perform best in terms of providing support, risk monitoring, risk comment and risk report. It is easy to use the model based on findings from the questionnaire. The process model is easy to learn, and there is no problem using the system in identifying risk, making decision decisions, treating and monitoring of risk. The process model is supported with risks' knowledgebase. Extending the model and making it an expert model which provides advice in making risk mitigation more flexible and simple. Lastly the process model is less complex, easy-to-use, efficiency, and less time consuming than existing risk mitigation model.

7.0 CONCLUSION AND FUTURE WORKS

This paper proposed a process model that codifies knowledge by using previous risk mitigation as reference based on the preferences of ICT practitioners and experts. A knowledgebase has been incorporated into the process model so that les experienced ICT practitioners and decision makers may refer to risk event histories of previous risk mitigation to make estimations on how to mitigate risk. Data was collected via the review of existing literatures on risk mitigation and knowledge approaches and knowledge codification practices.

Although ICT practitioners claim they mitigate risks in their organisations, there is evidence that they do not mitigate the identified risk systematically due to the high magnitude of loss caused by operational, technical and strategic risk associated within ICT. Thus ICT practitioners need to improve not only their ability to identify, but also to mitigate these risks associated in ICT infrastructures. Since one of the most powerful tools in mitigating risk in ICT is knowledge. There is need for ICT practitioner to codify knowledge, especially through the development of policies and practices to guide decision makers in mitigate operational, technical and strategic risk in their organisations. Thus the proposed process model provides adequate data from past risk mitigation project that can be used to mitigate present risk. The knowledge from past cases is codified and is re-used to mitigate risk in ICT. The process of codification can be used to share knowledge collectively and to transfer it at a minimal cost among the practitioners in the firm. The proposed model can also be used to maintain risk knowledge. The proposed model can also be as a decision support model that can be used by the professionals to quantify risk ratings.

The advantage of the model is that it can provide guidance for a firm about the risk and how the risk will be mitigated, according to past experiences. Another potential advantage is the model can be utilized as an organizational learning model. As the experiences of practitioners are captured, codified and saved in the enterprise knowledgebase, other practitioners can refer to this risk information while mitigating risk in a similar ICT project. The model was validated using questionnaire, which was used to collect data from six different Malaysian organisations. Future work will be aimed at implementing a risk mitigation system based on the developed process model. The risk mitigation system will be developed as a web based system.

Acknowledgement

We are grateful for the ministry of education Malaysia for their financial support for this research.

References

[1] Noraini, C. P., Bokolo, A. J., Rozi, N.H. N. and Masrah, A.A. M. 2015. Risk Assessment of IT Governance: A Systematic Literature Review. Journal of Theoretical and Applied Information Technology. 71(2): 184-193.

[2] 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.

[3] Peter, T. and Kevin C. D. 2012. Knowledge risks in organizational networks: An exploratory framework. Journal of Strategic Information Systems. 21(1): 1-17

[4] Bruce, E.P. 2007. A Strategic Risk Approach To Knowledge Management. *Business Horizon*. 50 (1): 523-533.

[5] Pratim, D. and William, A. 2010. Software And Human Agents In Knowledge Codification. Knowledge Management Research And Practice. *Operational Research Society*. 8(1): 45-60.

[6] Acelya, E. Y., Irem, D., Talat, M. B., Kerem, E., Selcuk, A. 2014. A Knowledge-Based Risk Mapping Tool For Cost Estimation Of International Construction Projects. *Automation In Construction*. 43 (1): 144-155.

[7] Jean, C.L.C. 2005. Are Organisations Too Complex To Be Integrated In Technical Risk Assessment And Current Safety Auditing. *Safety Science*. 43 (5): 613–638.

[8] Milan, R. and Petr, T. 2011. Operational Risk. *Scenario Analysis Prague Economic Papers*. 1(1): 23-39.

[9] Frits, T. and Chris S. 2013. Operational Risk Assessments By Supply Chain Professionals: Process And Performance. *Journal Of Operations Management*. 31(2): 37–51.

[10] Mark, L. F. and Richard J. A. 2011. What Is Strategic Risk Management? *Strategic Management*. 1(1): 1-20.

[11] Alexander, R., William, W. and Neil M. 2012. Strategic Risk Management, Edinburgh Business School, *Heriot-Watt University Edinburgh*. 1-15.

[12] Wendy, L. C. 2003. A Knowledge-Based Risk Assessment Framework for Evaluating Web-Enabled Application Outsourcing Projects. *International Journal of Project Management*. 21(2): 207-217.

[13] Nonaka, I. and Takeuchi, H. 1995. The Knowledge Creating Company: How Japanese Companies Create the Dynamics of Innovation. *Oxford University Press USA*. 1-15.

[14] Dale, N. 2005. Managing Corporate Risk Through Better Knowledge Management. *The Learning Organization*. 12(2): 112-124.

[15] Chris, K. 2013. Knowledge Management, Codification and Tacit Knowledge. *Information Research*. 18 (2): 1-14.

[16] Paul, W., Marcin, R., Dagmar, C., Milos, C., Jana, S. and Jana, M. 2014. The Implications of Tacit Knowledge Utilisation within Project Management Risk Assessment. 1(1): 645-652.

[17] Dani`ele, B., Gilles, L., Blandine, L.,Christophe, L. and Jocelyne, L. 2001. Completion Of Knowledge Codification: An Illustration Through The ISO 9000 Standards Implementation Process. *Research Policy*. 30(2): 1395–1407.

[18] Sandra, M. N., Carlos, E. S. S., Valério, A. P. S., Aneirson, F. S., Bárbara, E. P. S. 2014. Risk Management In Software Projects Through Knowledge Management Techniques: Cases in Brazilian Incubated Technology-Based Firms. *International Journal of Project Management*. 32(1): 125–138.

[19] Mostafa, J., Jalal, R., Mohammad, M. M. and Atefe, H,. 2011. Development And Evaluation Of A Knowledge Risk Management Model For Project-Based Organizations. *Management Decision*. 49(3): 309-329.

[20] Eduardo, R. and John, S. E. 2009. Knowledge Management and Enterprise Risk Management Implementation in Financial Services. 1(1): 1-17.

[21] Noraini, C. P. and Bokolo, A. J. 2015. A Review on Decision Making of Risk Mitigation for Software Management. *Journal of Theoretical and Applied Information Technology*. 76(3): 333-341.

[22] Noraini, C. P., Bokolo, A. J. and 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, 1-6.