Conceptual Framework on Risk Management in IT Outsourcing Projects

SYARIPAH RUZAINI HJ SYED ARIS, NOOR HABIBAH ARSHAD, AZLINAH MOHAMED
Faculty of Information Technology and Quantitative Science (FTMSK)
Universiti Teknologi MARA
Selangor
MALAYSIA
syaripahruzaini@yahoo.com, habibah@tmsk.uitm.edu.my, azlinah@tmsk.uitm.edu.my

Abstract: - Outsourcing is becoming a trend nowadays. Malaysia also takes this opportunity and embraces in IT outsourcing. As a result, Malaysia has been ranked as the third most attractive destination for outsourcing after India and China. Despite increasing number of organizations that involve in IT outsourcing, it should be noted that IT outsourcing is not a panacea. It comes together with risks. The risks, if not managed, will lead to outsourcing failure. Even though other areas have adopted risk management as their patching material, the application of risk management in IT outsourcing was not quite accomplished. Risk management should be conducted in IT outsourcing as it will foresee risks that might disturb the smooth flowing of IT outsourcing and prevent or reduce the impact of risks if they occur. It should be conducted at early stage and should be continuously performed until the end of outsourcing life cycle. This paper presents a conceptual framework to manage risk in IT outsourcing. The framework will cover the process in risk management in IT outsourcing as well as the risk management principle that should be conducted at each and every phases of IT Outsourcing life cycle. A set of questionnaire was distributed to organizations to validate the conceptual framework. The findings showed that the consequences of not practicing risk management would result in poor controlling and managing of IT outsourcing projects. Based on the findings, future empirical and exploratory survey will be conducted and risk management in IT outsourcing framework will be developed.

Key-words: - Risk Management, Malaysia, Analysis of Decision to outsource, Selection of Service Provider, Contract Management, On-Going Monitoring.

1 Introduction

Outsourcing is one way for the government to operate more effectively while saving money [45]. Therefore, Malaysian government has actively involved and supported the idea for outsourcing. As reported by Ministry of International Trade and Industry (MITI), Malaysia was ranked as the third most attractive destination for outsourcing after India and China [2]. Malaysia has all it takes to attract organizations to invest in outsourcing. The infrastructure is robust ane the fiscal/tax/regulatory environment is sound and affordable [10]. Recently announced, large IT outsourcing contract includes Maybank with RM 1.3 billion deal, Malaysia Airline System Berhad (MAS) with RM 440 million deal and Permodalan Nasional Berhad (PNB) with RM 32 million extension contract and the general trends towards IT outsourcing would continue [9].

IT outsourcing is not a panacea, not all projects end up successfully. In Malaysia for example, only 9.2% projects that engaged in IS development succeeded [39]. Therefore, many researchers have come out with ways to successfully manage the outsourcing activities, but there are still not many discussed IT outsourcing with great details. Most of them are anecdote and have no empirical validation. Most of the discussions only enhanced the governance to successfully manage the IT outsourcing project. However, it should be noted that there are two approaches to achieve project success; project management and risk management [41]. Therefore, this research focuses on the contribution of risk management to the success of IT outsourcing.

Previously, the application of risk management in IT projects was not seriously considered. However, now it is gaining its popularity and is seen as a useful patching material to fill the project management fissure and strengthen its surrounding walls [26]. Nevertheless, even though the importance of risk management in IT outsourcing is realize, the application is still low [26]. The low practice and application of risk management was also confirmed by a research done in [59]. Another research done showed that only 8% of IS project

integrate risk management in the development process due to no formal training in risk management [36,37,38].

This paper adopts risk management perspectives into IT outsourcing life cycle and proposes a framework that is also theoretically supported. As shown through the pilot study, the risk management in IT outsourcing conceptual framework contributes to reduce the risk in IT outsourcing life cycle. This paper first presents some discussion on IT outsourcing, the reference theory and risk management. The conceptual framework is then presented. In order to evaluate the framework, a pilot study is conducted. The findings are then discussed.

2 IT Outsourcing

IT outsourcing is an act of delegating or transferring some or all of the IT related decision making rights, business process, internal activities and services to external providers. Providers will develop, manage and administer these activities in accordance with agreed upon deliverables, performance standards and outputs, as set forth in the contractual agreement [53].

In Malaysia, IT system and business processes are increasingly being outsourced. As surveyed by NISER [33], in government sector, the system or processes most commonly outsourced are ISP website hosting followed by ICT application maintenance and support, ICT infrastructure, application service provision, ICT security audits and security policy or standards development.

In IT outsourcing, it is important to manage the outsourcing activities effectively and choosing the right service provider for the job. A good service provider will be able to improve the quality of security in a highly cost-effective way, because it is its core business activity to do so. On the other hand, outsourcing to a poor service provider may increase risks [33]. Therefore, many researchers try to come up with ways to successfully manage the outsourcing activities, but there are still not many proper guidelines that touched IT outsourcing with great details. Most of the researches has only focused on why, how and what do firms outsourced, the client vendor relationship and the factors influencing the outsourcing success [57]. Only few literatures that emphasize the importance of risk management in IT outsourcing. Thus, this paper presents a conceptual framework to manage IT outsourcing projects.

The conceptual framework proposed here relies mostly on Transaction Cost Theory, Agency Theory and Relational Exchange Theory. Transaction Cost Theory tackles the problem of deciding whether to outsource or not. Relational Exchange Theory tackles the problem of relationship development process in order to select service provider. Agency Theory tackles the problem of managing the contract and at the same time ensuring the goal of IT outsourcing are met. The details of each theory will be discussed in the next section.

2.1 Reference Theory

Many researchers have come up with the process of managing IT outsourcing [11,13,48,50,56]. However, some questions arose [30]. The questions are as follows.

1. How to determine the decision to outsource and the function to be outsourced?
2. How to choose appropriate service provider for outsourcing?
3. How to design and manage the contract that will govern the outsourcing agreement and how to best maintain the relationship and at the same time ensuring the goal of outsourcing is met?

Nevertheless, the questions can be answered by adopting theories as discussed below.

2.1.1 Transactional Cost Theory

Transaction cost theory (TCT) is the economic theory used in order to decide whether to outsource a function or not. TCT implies total cost which consists of production cost and transaction cost. Production cost is the cost to produce the transaction meanwhile transaction cost is the cost to control and monitor worker. Transaction cost or also known as coordination cost consists of cost of monitoring, controlling and managing transaction.

Williamsons [40] assumes that markets provide cheaper production cost than hierarchies through economic of scale. However, it causes higher coordination cost. Therefore, transaction cost theory uses four constructs to determine which governance structure is more appropriate for cost reduction. The four constructs include cost, transaction type, threat of opportunism and uncertainty.

The cost constructs indicate that for market governance structure, the production cost is low but the coordination cost is high. On the other hand, the hierarchies governance structure, indicates high production cost and low coordination cost. The

transaction type construct includes the identification of frequency (how often transaction occurs) and asset specificity (degree of customization of the transaction).

The third construct, threat of opportunism indicates that people act in their own self-interest, where they may not always be trustworthy, honest or purport fair representation. However, this construct is only a treat when there is a small number of vendors due to a limited choice. Even so, this threat can be reduced by signing a complete contract. Performing a transaction under high uncertainty is very costly perhaps even impossible. However, the organization can sacrifice design features to make the transaction more standardized, or surround the transaction with elaborate contract or even produce the transaction internally.

2.1.2 Agency Theory

Specifically, Agency Theory (AT) is directed at the ubiquitous agency relationship, in which one party (the principle) delegates works to another (the agent), who perform that work [24]. This theory concerns with resolving two problems that might arise with agent relationship. The first problem concerns with the principle that cannot verify that agent has behaved appropriately due to different goals and it is expensive to verify what the agent is doing. The second problem concerns with different attitude towards risks as each of them prefers different action.

The attempt of the theory is to describe the principle agent relationship using metaphor of a contract. The focus is to determine the most efficient contract governing the principle agent relationship. Agency Theory must help to answer the following questions; what can the principle do to encourage quality services and fair treatment by the provider and what can the provider do to keep the user satisfies and at the same time to reach its own outcome goals [30].

2.1.3 Relational Exchange Theory

Relational Exchange Theory (RET) is based on relational norms. Relational norm is the key to determine the efficiency of contract governance between the parties involved in transaction [42]. The dimensions of relational norms include flexibility, information exchange and solidarity. Flexibility refers to willingness to make adaptations as circumstances change. Information exchange indicates that parties will proactively provide information useful to the partners, meanwhile solidarity is high value that is placed on the relationship.

Table 1 shows how theories mentioned above help in resolving the questions and concerns in IT outsourcing. Table 1 shows how questions arose by some researchers which can be answered by adopting a particular theory and the rational behind it. Logan [30] has issued some questions concerning IT outsourcing life cycle. The questions include how to determine the decision to outsource and the function to be outsourced. Those questions can be answered by adopting TCT where it helps in terms of deciding whether to outsource a function or not and the function that should be outsourced [3,27,40,42,55,61].

Table 1: Questions arise and the supporting theories.

Question arise	Supporting theories and the rationale	Outcome
How to determine the decision to outsource and the function to be outsource [30]	TCT resolve the conflict of whether to outsource or remain the function in house as well as determining which function to be outsourced [3,27,40,42,55,61]	Decision to outsource and the function to outsource
How to choose for appropriate provider for outsourcing [30]	RET helps to resolve the conflict by suggesting relationship development process which will help the process of knowing future provider [3,13,42]	Selection of appropriate service provider
How to design and manage the contract that will govern the outsourcing	Agency theory help by designing the types of contract and relationship that is necessary to provide and support an environment of trust [24,27,30,42]	Contract manage-ment
How to best maintained the relationship and at the same time ensuring the goal of outsourcing is met [30]	Agency Theory answer the following questions; what can the principle do to encourage quality services and fair treatment by the provider and what can the provider do to keep the user satisfies and at the same time reach its own outcome goals [24,27,30,42].	Monitoring the relation-ship

Another concern by Logan [30] was how to choose for appropriate service provider for outsourcing arrangement. In this particular question, RET helps by suggesting relationship development process to understand future service provider

[3,13,42]. Another question arose includes how to design and manage the contract that will govern the outsourcing. AT helps this issue through designing the type of contract and relationships that is necessary to provide and support the environment of trust [24,27,30,42].

Next concern includes how to best maintain the relationship and at the same time ensuring the goal of outsourcing is met [30]. Agency Theory is used because it answers this questions; what can the principle do to encourage quality services and fair treatment by the provider and what can the provider do to keep the user satisfy and at the same time reach its own outcome goals [24,27,30,42].

Previously, the application of risk management in IT outsourcing were not quite accomplished. Recently, the importance of risk management is realized. Instead of focusing on the project management part, risk management focuses on the issues and risks that might effect the smooth flowing of IT outsourcing arrangement.

3 Risk Management in IT Outsourcing

There are two approaches to achieve project success; project management and risk management [41]. Therefore, instead of focusing on the bright sight of a project as suggested in project management, risk management focuses on the issues and risks that might appear during a lifetime of a project. In outsourcing arrangement, the risk is higher as more players involved. Since the IT outsourcing trends in Malaysia would continue, it is important to enhance and manage the risk that might derive. This risk should be managed as failing to do so will invite disaster to organizations. Therefore, organizations should conduct careful and deliberate risk management as it can substantially attenuate the level of risks exposure [20].

Consorting with adapting risk management in IT outsourcing practices, McCormack [44] in his report of Financial Service Authority (FSA) Approach to the Supervision of Outsourcing outline six key phases to review the outsourcing process. They are as follow.

1. Strategic decision to outsource
2. Due Diligence process.
3. Contract and service level agreement
4. Change Management
5. Contract Management
6. Exit strategies and contingency plan.

Funk et al. [17] had emerged a new approach to manage risk in IT outsourcing. According to them, there are four layer of sound risk mitigation in the IT outsourcing context. They are :

1. Mitigating risks in day-to-day, normal operations
2. A sound structure for addressing serious unexpected operational problems
3. Advance planning for the end of the outsourcing relationship
4. Providing in all cases for the financial protection of the organizations.

FFIEC [15] comes up with a process of risk management in IT outsourcing. The process consists of four steps namely risk assessment and requirement definition, due diligence in selecting service provider, contract negotiation and implementation and on-going monitoring.

In addition to performing risk management, it is important to perform it in the earlier stage [47] so that the risks can be foreseen and be prevented or at least reduce the impact of the risks if they occurred. However, early identification of risks is not enough. During the initial stage, risk assessment may not be imprecise due to limited information and resources. Therefore, organizations should have systematic risk management and continuously carry it out through the life of the project [52].

Many studies proved the practice of risk management will increase the likelihood of a successful project including a survey done to show a positive association between risk management and project success [35]. Therefore, risk management should be recognized as one of the critical success factors in IT outsourcing projects. In Malaysia, even though the awareness of risk management is high, the practice is still low. The low practice and application of risk management were also confirmed by a research in [59]. Another research done showed that only 8.0 percent of IS project integrate risk management in the development process due to no formal training in risk management [36,37,38]. Therefore, this paper presents a conceptual framework that discusses the phases of risk management in IT outsourcing. The conceptual framework takes into consideration the elements that should be conducted during the outsourcing arrangements as well as the elements that should be performed at each IT outsourcing life cycle to reduce risks.

4 Methodology

There are two methodologies used in this paper. The first is reviewing secondary data in order to develop the conceptual framework. Then, a set of pilot questionnaire was distributed to 15 organizations with ten returned answers to validate the conceptual framework.

5 Conceptual Framework on Risk Management in IT Outsourcing

Many researchers have come up with risk management in IT outsourcing framework. However, most of them are anecdote and have no empirical validation. Therefore, this paper proposes a conceptual framework that is theoretically supported and empirically validated.

The overall conceptual framework illustrates a continuous risk management throughout the life cycle of risk management in IT outsourcing projects. The inner layer of the conceptual framework presents risk management principle. The risk management principle will identify, assess and manage risk. Corresponding with the application of risk management in IT outsourcing, it will identify and manage risk routinely throughout all phases of the risk management IT outsourcing's life cycle as presented with the outer layer.

Figure 1 : Conceptual Framework of Risk Management in IT Outsourcing

The outer layer; risk management in IT outsourcing phases, takes into consideration the questions arise in IT outsourcing that has been answered by the supported theories as shown earlier in Table 1. Therefore, these phases are more reliable since they are also supported by theoretical background. While the process of IT outsourcing ensures the organization gain benefits from the projects, risk management process will help to recognize and reduce the risk.

The conceptual framework proposed is as shown in Figure 1. The detail description for each layer is discussed in the next section.

5.1 The inner layer: Risk Management Principle

The inner layer; the risk management principle is the basic process of managing risk. Charette [52] has come up with risk management process. He divided risk management into two parts namely risk analysis and risk management. The steps suggested by Charette are similar to those described in most discussions of risk management [31,32,34,41]. The risk management principle can be pictured as Figure 2.

As suggested by most of the researchers, risk management process can be divided into two main phases. Each phase comprises several factors as described below.

5.1.1 Factors in Risk Management Principle

Risk assessment is a process where the organization identifies, analyze and prioritize the risk. During the risk identification process, the organizations identify all risks that might disturb the smooth flowing of the outsourcing process. Risks identified should include threat and vulnerability from all aspect. Committee should list comprehensive risk [32,43,52] from any perspective from their point of view. However, it is important to note that the risks should be bounded by the scope of the project itself so that they will not waste their time trying to address the risks that is outside their scope [43].

After the list of risk is complete, it is important to identify the current control available to manage the risk [34]. It is important to identify the current control because this action can determine whether the current action is appropriate to address the risk or not. If the current control is proven ineffective, the committee then can figure out new ways to address the risks or maybe enhance the current control.

In risk analysis phase, the organizations analyze the risk by including the probability of occurrence and the impact of the occurrence [32]. The probability and the impact of the risks occurrence will be quantified as high, medium and low.

Once the risks have been identified and analyze, risks will then be prioritized based on probability and impact analysis. From the risk prioritization, the committee will recommend control to mitigate and

manage the risks. One way of doing this is by performing CBA to select the best control option that suits their current condition. All the work done is documented and report is produced and submitted to risk management co-ordinator. The report is called Risk Management Planning (RMP).

Risk treatment is a phase where the organization actually implements the action to manage the risks. There are four steps taken in order to make sure the control taken is really efficient to manage the risk. It starts with evaluation. After the committee has decided and recommended the action necessary to manage the risks, the RMP is submitted to the risk co-ordinator. Here, they will evaluate the risks prioritizing [8], the recommended control option and the CBA.

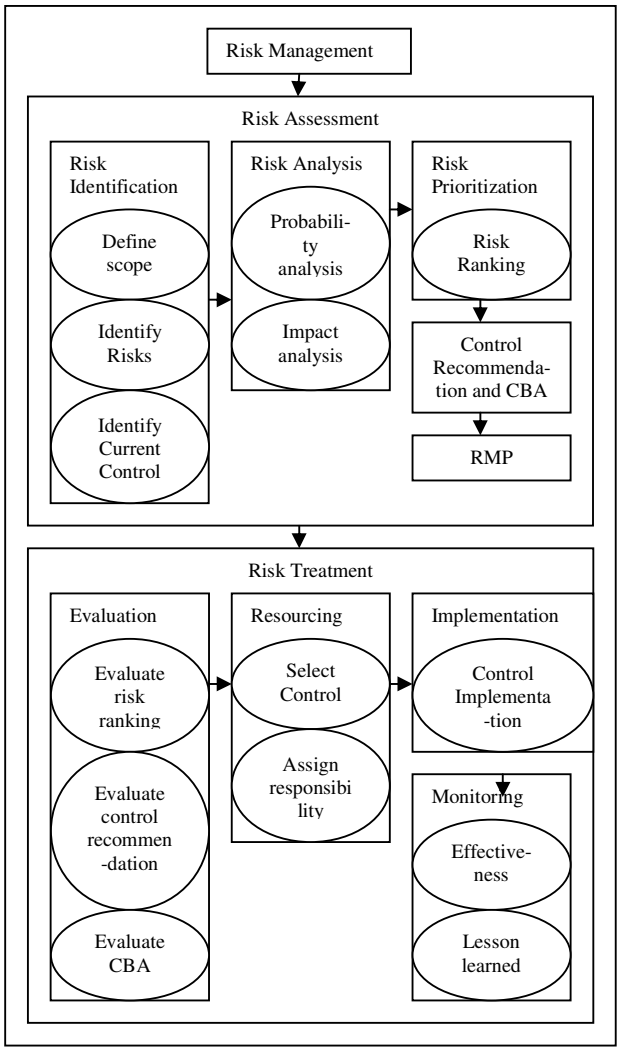

Figure 2: Risk Management Process
Source: Syaripah Ruzaini et al. [58]

In the resourcing phase, the co-ordinator will select the control based on the CBA done previously [8]. The co-ordinator will then assign the personnel that are responsible to address the risks by performing specific action selected. The new information will be added to RMP.

In the implementation phase, the RMP which consist of the type of the risks, control to be taken to manage the risk, the CBA of the control and personnel assign will be implemented.

The final step in risk treatment is monitoring. During this phase, the committee will monitor the action taken to measure the effectiveness of the control taken to manage the risks. They will then provide lesson learned.

Risk management should be treated as a continuous process. It should be performed at each life cycle in IT outsourcing arrangements. This is because initial risk management might not contain enough information on risk that might occur over time. By time, another new risk might appear, so that it is important to keep conducting risk management.

5.2 The Outer Layer: Risk Management in IT Outsourcing Process

Risk management in IT Outsourcing process consists of four main phases. The first phase is Analysis of Decision to Outsource. In outsourcing, this step concerns with the decision whether to outsource or not and the function that should be outsourced. CBA should also be conducted in order to determine the cost and benefit of performing outsourcing arrangements. In consorting of risk management into this process, risks associated with outsourcing activities are determined. The outcome of this phase is the decision to outsource and the function to be outsourced as well as the risks associated with outsourcing activities.

In Selection of Service Provider, it is important to select service provider that will best suit the organization's need and is able to deliver what is promised. Adopting risk management into this phase will ensure organization select service provider with good background so that the risks of opportunism can be reduced.

Contract management is a phase where organization should design and manage the contract that will govern the outsourcing project. By adopting risk management, organization should negotiate a contract so that the entire requirement is clearly stated and written. The purpose of on-going monitoring is to maintain relationship and at the same time to ensure the goal is achieved. By

applying risk management, the organizations should monitor service provider to make sure it delivered upon a contract agreement.

Table 2: How IT Outsourcing and Risk Management concerns fit in the process

RM in IT Outsourcing process	Concerns	Outcome
Analysis of decision to outsource	*ITO:* To decide whether to outsource or not and function to be outsourced and CBA of performing those action *RM:* To determine risk associated with outsourcing activities	Decision to outsource and the function to be outsourced as well as the risk associated with outsourcing activities
Selection of service provider	*ITO:* To select service provider that will best suit the organizations' needs and able to delivers what is promised *RM:* To select service provider with good background so that the risk of opportunism can be reduce	Selected service provider
Contract management	*ITO:* To design and manage the contract that will govern the outsourcing project *RM:* To negotiate a contract so that all the requirements are stated and written clearly	Clearly written contract
On-Going monitoring	*ITO:* To maintain relationship and at the same to ensure the goal is achieved *RM:* To monitor and ensure the service provider delivers what is promised	Monitoring the work of service provider to make sure they deliver what is promised.

Once the contract end, the organization can either renew the contract of the same function with the same service provider by signing a new contract agreement, or choosing another service provider to continue performing the same function by selecting a new service provider.

Table 2 shows how the concerns of IT outsourcing and risk management fit in risk management in IT outsourcing process.

5.2.1 Phases in Risk Management in IT outsourcing process

Risk management in IT outsourcing process involves four main phases. Each has its own factors in order to achieve the goals and objectives at each phase. Te factors are discussed below.

Analysis of Decision to Outsource

McCormack [44] once mentioned that lack of research during initial phase can lead to a failure. Therefore, it is important to perform research during the initial stage to gather information on IT outsourcing and the risks of doing so. The factors that should be practiced in this approach are as illustrated in Table 3.

Table 3: Factors in Analysis of Decision to Outsource

Factors	Description	Ref
Select and Understand the Function to be Outsourced	Selection of function to be outsourced and understand it to ease the project management	11,49
Conduct Cost Benefit Analysis	The comparison between the cost and benefit of performing outsourcing activities	51
Setting up realistic scope, budget and schedule	Setting up goals to understand the objectives and the deliverables of the project	48,53
Determine the number of service provider	To ease the task of managing multiple service provider if the concept of multi-provider is applied.	7
Determine the type of relationship	To ease the process of contract designing	13,47
Risk Management committee creation	Committee creation to help foresee the risk	15
The involvement of stakeholder and risk management committee to assess risk and create RMP	Involvement of stakeholder to take in the risks from managers' point of view	15
Use RMP for the rest of outsourcing process	The usage of RMP to control and assess risks	15

From Table 3, it can be seen that the function to be outsourced must be understand. It has been cases where outsourcing fails because the organizations outsourced a broken function [11]. Gonzales et al.

[49] also mentioned that understanding the nature of the work being outsourced as a way to reduce risks in IT outsourcing.

Organizations then conduct Cost and Benefit Analysis (CBA) to compare the benefit and the cost of doing the function in-house versus outsourcing it to service provider. Then, organizations should defined realistic and achievable goals as it is critical risk factor [53] and failing to do so is one of the top reasons for IT outsourcing failures [48].

The determinants of number of service provider should be determined in this phase to ease the task of integration. As different type of relationship requires different type of contract and thus different type of management [13,47], it should be determine in this phase to ease the contract designing phase.

Risk management should be created in this phase as they will be responsible to foresee the risk in IT outsourcing. The involvement of stakeholder is also important to view the risks from managers' point of view. Risk management plan is then developed and is used to control and assess risk in IT outsourcing projects.

Selection of Service Provider

Ineffective service provider process has proven to increase risks in IT outsourcing (APICS, 2003) [1]. Therefore, in order to reduce risks, service provider should be selected carefully. Information gathered from previous phase is included in the Request for Proposal (RFP) [4]. It is then distributed to prospect service provider. Once the proposal is received, it is review against the organizations' need [4]. Service provider will then be evaluated in order to select the most suitable one. Factors that should be considered in order to select service provider are summarized in Table 4.

It is significant to find service provider with good reputation and performance as service provider's instability will open new door for risk [17]. Service provider's lack of experience can increase risk in outsourcing [54]. The experience of service provider over many projects allows it to select and combine the best and most effective practices from many organizations. Bragg [54] once mentioned that service provider that shows some financial problem on their financial statement should be avoided. This is because service provider with nothing to lose is more willing to walk away from the contract and declare bankruptcy [62].

Personnel assigned should be considered as factor in selecting service provider [6]. This is to ensure the integrity and expertise of the personnel assigned by service provider. Ramsaran [6] also suggested organizations to consider service provider with technology availability, adaptability and expertise to reduce risks. Choosing service provider that ally with standard is important as they will reduce risk in the future [6]. Therefore, this factor should be considered during selection of service provider.

Table 4: Factors in Selection of Service Provider

Factors	Ref
Reputation and Performance	17
Experience	54
Financial stability	54,61
Personnel assigned	6
Access and ability to adopt to latest technology	6
Practices of standard, policies and procedure	12,21
Practices of security	12,21
Responsibility towards disaster recovery plan	53
Usage of third party	25

One of the concerns in the security practices is the integrity of the information [12]. The obligation towards personal data privacy and security become even more critical when organizations are engaging in outsourcing [21]. Therefore, organization should review service provider that practices standard, policies, procedure and security in order to reduce risk.

Dhar and Balakrishnan [53] emphasized that loss of control over disaster recovery plan could contribute to risk. Therefore, it is important to select service provider that will be able to provide disaster recovery plan. The involvement of subcontractors will increase risks [25] especially if service provider makes their own decision regarding the usage of third parties and organizations is not informed. Therefore, before selecting service provider, it is important to know the service provider's usage of subcontractors.

Contract Management

Contract is the most important element of a secure outsourcing plan [6] and it must be recognized as important risk management vehicles [20]. Therefore, it is included in the approach to reduce risks. The phases practiced during contract management are as in Table 5.

In managing a contract, contract negotiation should be performed to ensure all needs and requirements are included. The engagement of legal counsel is important to review the contract. After contract designing is completed, contract will be sign. Organizations will then make sure service

provider meet the needs and requirements stated in the contract.

Table 5: Phases in Contract Management

Phase	Description	Ref
Contract negotiation	Negotiate a contract so that all need are included	50
The engagement of legal counsel	Engage legal counsel to help with the preparation of contract	15
Contract designing	Contract designing	50
Contract signing	Contract signing	50
Meeting the contract	Make sure the service provider meet the contract	5

On-Going Monitoring

On-Going monitoring is a continuous phase that takes action as soon as the contract is signed. It is important to make sure the service provider is monitored along the way of outsourcing activities. The goal of this phase is to make sure all the promises made during the contract negotiation is delivered. Performing on-going monitoring phase will enhance the ability to mitigate risks by identifying potential problems before it becomes catastrophic [28].

Once the conceptual framework developed, it is validated through a set of pilot study administered to ten organizations. The results of the study are discussed below.

6 Validation of Conceptual Framework with Current Practices

Table 6: Reliability Analysis for the Variables

Variable	No. of Items	Cronbach's Alpha
Factors practice in Analysis of Decision to Outsource	10	0.874
Factors practice in Selection of Service Provider	12	0.647
Phases practice in Contract Management	5	0.884
Factors in Risk management principle	20	0.939

After data collections were completed, the variables were tested to see their reliability. The findings show that the variables have alpha value greater than 0.60 which indicate that all the variables are consistent and reliable. Details of the reliability analysis are as tabulated in Table 6. Based on the data gathered from the questionnaire, the following findings and discussions are presented in the next section.

6.1 Organizational background and project characteristics

The research involved ten organizations to measure their risk management practices. The designation of the respondents are Project Director, Principle Assistant Director, IT Manager, three System Analysts and four IT/IS officers. From ten of the organizations, five involve in services, three in health care, one in human resources and another one is a law enforcer. Six organizations outsourced their application system development functions, two organizations outsourced their ICT application maintenance, one organization outsourced its ICT infrastructure and one organization outsourced its strategic planning. The project cost is range from 50K to 20M (Ringgit Malaysia).

All government agencies agreed that the reason they outsourced a particular function is the resources and expertise are not available in-house. Surprisingly, cost reduction is not the main reason to outsource a function in government agencies. This might support the research where cost reduction is a goal of traditional outsourcing and therefore might not be appropriate in current environment [16]. Other reasons to outsource include to focus on core business, to improve productivity, to achieve higher quality, to achieve higher customer satisfaction and government support. From the ten organizations surveyed, only one organization involved the use of multi-vendor to complete the task. Six out of ten organizations focused on selective outsourcing. Selective outsourcing is the decision to outsource selected IT functions to service providers while still providing between 20% and 80% of the IT function internally [22]. The rest of the organization performed total outsourcing.

Six of the organizations set up strategic partnership type of relationship. The rest of the agencies set up buyer/seller relationship arrangement. All organizations sign fee-for-service contract. Fee-for-service contract is divided into four types, namely standards, detail, loose and mixed [19]. From the four types of contract, seven organizations signed detailed contract while the rest signed for standard contract. From 10 organizations that participated in the survey, only one signed for medium-term (from 6-10 years). The rest of the respondent signed for short-term contract (less than 5 years). This is because of the policy that provide five years license contract which subject to satisfactory review of performance.

6.2 Risk Management Principle

Risk management principle is the core practices in the framework. The risk management principle suggested factors that should be considered during each and every phases of IT outsourcing life cycle. Table 7 shows how organizations practiced risk management principle.

Table 7: Risk Management Principle

Risk Management Principle	Hit
Definition of scope of risks	9
Risk Identification	9
Identification and evaluation of the effectiveness of current control	9
Selection of control	9
Assign of responsibility	9
Implementation of control	9
Continuous review/feedback on risk management strategies and performance	9
Regular reporting to senior management	9
Risk Prioritization and selection of risk that need active management	8
Control recommendation	8
Control effectiveness measurement	8
Provide lesson learned	8
Probability analysis	7
Impact analysis	7
CBA of addressing risk	5
Risk Management Plan (RMP) documentation	3
Risk ranking evaluation	3
Control recommendation evaluation	3
CBA evaluation	1

Table 7 shows that nine organizations performed the initial stage of risk management such as definition of scope of risk, risk identification, identification and evaluation of the effectiveness of current control. Scope of the risk should be identified to ensure the process of risk identification is encapsulated. Risk is then identified using tools such as brainstorming and checklist. Current control is then identified and evaluated to measure its effectiveness on the risk. If the control is not effectives, new control will be suggested. From this finding, it is a good sign to show organizations are starting to realize and apply risk management as part of their practiced.

However, from Table 7, it can be seen that some organizations did not conduct probability analysis and impact analysis. Only half of the organizations conducted CBA of addressing risk. Table 10 also shows only three organizations create risk management plan. They also did not performed principles that need them to evaluate things such as the risk ranking, control recommendation and CBA evaluation. This might due to these principles requires specific skills, technique and task. Other principles are fairly practiced.

From the findings, it can be concluded that most of the organizations still skip most of the principles that involve specific skills, techniques and tasks. This support the earlier findings that mentioned organizations did not conduct risk management due to no formal training [36,37,38]. It can be concluded that organizations have realized the importance of risk management, but it is not a norm in organizations due to lack of knowledge and skills. These findings support the research by [26] which stated that the awareness of risk management is high but the level of practices is still low.

From the findings, there is a need to develop risk management in IT outsourcing framework to assist organizations with their risk management practices. Risk management should be stressed as the outmost important ways for a project to be successful.

6.3 Risk Management in IT Outsourcing Process

Based on the conceptual framework proposed earlier, the risk management in IT outsourcing can be divided into four main phases. The finding and discussion are as described below.

6.3.1 Analysis of Decision to Outsource

Creating a risk management committee is the first step in risk management. In order to incorporate risk management practices, it is utmost important that the stakeholder be part of risk management committee and create Risk Management Plan (RMP) to control an outsourcing action. This team is crucial as it will be responsible in identifying and managing the risks.

However, only three organizations in the survey follow these procedures. This is an early sign that IT outsourcing projects in Malaysia did not fully practice risk management. The reason given for not creating risk management committee is that risk management is not the practice in their organizations.

Then, organizations should consider factors listed in Table 3. However, Table 8 shows how organizations in Malaysia practiced factors that should be performed during the early phase of IT outsourcing.

The survey shows that 9 organizations conduct analysis of decision to outsource. One organization skip this process as the project is a directive and the organization will only be responsible with the next

phase of IT outsourcing life cycle. It is a good practice when all organizations carefully select and understand the system function before it is passed to the third party so that the requirements can be easily determined. This can eliminate the myth of project management where client do not know what they want. Once the system function is fully understood, they can clearly state their needs and requirements to the service provider.

Table 8: Factors considered during the analysis of decision to outsource phase

Factors Considered	Hit
Select and Understand the function to be outsourced	9
Cost Benefit Analysis (CBA)	8
Setting up realistic scope, budget and schedule	9
Determine the number of service provider	2
Determine the type of relationship	5
Risk management committee creation	3
Involvement of stakeholder in the Risk management Plan (RMP)	3
Usage of the RMP in monitoring the IT outsourcing process.	3

CBA is then conducted in order to compare the benefits and the costs of doing the function in-house versus outsourced. However, one organization did not perform CBA. In this particular agency, CBA is not a high priority as the project is a mandatory project where the success of the development of the project outweighs the cost.

After the decision to outsource has been finalized, organizations defined realistic and achievable goals which include realistic budget allocation, specification of scope requirement and schedule of the project. Failing to do so is one of the top reasons for IT outsourcing failures [60]. Therefore, by defining realistic and achievable goals, risks of failure are reduced.

The previous literature mentioned that usage of multi-vendor could minimize the risks of IT outsourcing [11]. However, in the survey, only two organizations practiced the usage of multi-vendor concept because of the complexity and size of the projects. Managing the relationship is very important to ensure the success of IT outsourcing. Half of the agencies therefore signed for strategic alliance type of relationship to ensure the good relationship between the agencies and service provider.

By conducting analysis of decision to outsource, it shows that the organizations have included risk assessment in their project. Since risk assessment during the earlier phase might not be adequate as organizations have limited information, organizations should continuously conduct risk management in all IT outsourcing life cycles to foresee new risk that might put the project at stake.

6.3.2 Selection of Service Provider

Proper selection of service provider is necessary to reduce the risk of IT outsourcing [1]. In outsourcing arrangement, it is important to find service provider with the right mix of operating style, reputation, experience and price than to pick just based on the lowest bid price.

Request for proposal (RFP) should be prepared using the information gathered during the analysis of decision to outsource phase. After receiving the proposal, it should be evaluated against the organizations' needs.

As stated previously, there are several factors that should be considered in evaluating service provider. The factors that were considered are as tabulated in Table 9.

From the survey, reputation and performance are the most important criteria in selecting service provider. The high reputation and good performance of service provider will ensure high reliability of services and products. The organizations also need to consider the experience of service provider with the function being outsourced. With a team of experienced IT personnel, the service provider could deliver high quality products.

Financial stability is another criterion that is considered important. This will also ensure that the service provider may not drop a project or go out of business. The organizations are also interested with the provider that has access and ability to adopt to latest technology. This is to make sure that any upgrading or integration is easily performed in the future.

Table 9: Factors considered during the service provider selection process.

Factors considered	Hit	Rank
Reputation and performance	10	1
Experienced with the function	9	2
Financial stability	8	3
Access and ability to adopt to latest technology	8	4
Practices of standard, policies and procedures	7	5
Practices of security	7	6
Responsibility towards disaster recovery plan	7	7
Personnel assigned by service provider	6	8
Usage of third party	4	9

Practices of standard, policies and procedure were also ranked high because most of the project involves confidential information. What is concerned most during dealing with outsider is its trustworthiness towards the confidentiality of the information. In outsourcing, most of the confidential information is available to the provider. Therefore, it is important to make sure those information does not being misused by the provider thus to prevent any problem in the future.

The organizations also considered provider that will provides disaster recovery plan. This is because most of the projects outsourced are crucial and it is important for business to be recovered from major disaster. The Total Hospital Information System (THIS) for example, involves critical system where the system cannot even afford to have a down time as the patients' information travel from one section to another section each and every second. Even if system failure occurs, the existence of disaster recovery plan can be used as a backup to the system.

Screening personnel background is also important in selecting service provider so that no conflict of interest occurs especially with the appointed subject matter expert by the service provider. The subject matter expert chosen must not by right have any relationship with the organizations.

The usage of third party was the least important criteria in selecting service provider as not many providers used the subcontractor services. The organizations should also perform site visit at their service provider location to have an overview of its working environment. However, only three organizations performed the site visit evaluation as the other organizations have faith with their provider.

6.3.3 Contract Management

A research done showed that the highest risk in ICT outsourcing is providers who do not comply with contract [39]. Therefore, contract should be seen as the most important element of a secure outsourcing plan [6] and it must be recognized as important risk management vehicles [23]. Phases considered during contract management are shown in Table 10.

During the contract management phase, it is important to negotiate a contract so that all needs and requirements are defined clearly. From the survey, almost all organizations conducted contract negotiation. The engagement of legal counsel is important as they can help in reviewing the contract and this is a common practice at most of the agencies.

Table 10: Phases considered during the contract management.

Phases Considered	Hit
Contract negotiation	9
Legal Counsel engagement	9
Contract designing	9
Contract signing	10
Meeting the contract	9

In IT outsourcing, it is important to include Service Level Agreement (SLA) in the contract as it will provide a formal agreement regarding the division of work between the organization and the service provider. The contract should include scope, cost and durations to complete the projects, description of relationship, penalty and rewards for higher or lower performance, security and confidentiality of the organization resources, control over the projects, type of report the organizations should receive, the service provider's responsible towards the recovery plan and subcontracting, ownership and license, dispute resolution, limitation of liability, termination clause and regulatory compliance [13].

After designing and signing the contract, the next step is to make sure that the agreed contract is met [6]. All the organizations' requirements are already built into the contract. Therefore, service provider has to comply with the contract.

Almost all elements that are required in a contract as stated in [13] are presented in the organizations' contract. However, some of them did not include the dispute resolution, limitation of liability and regulatory compliance part. This is because they are singing standard contract which was prepared by the provider. Standard contract has limitation; most of off-the-shelf contract is limited in specification and requirement. Therefore organization cannot make any changes without being charged by the provider.

From ten organizations involved in the survey, one admitted that the cost stated in the contract was higher than the estimation, two organizations declared the schedules were not met and one case of the unmet SLA. The organization that faced overrun budget problem also admitted that it has less control over the project. Besides that, problem cited include reports not received on time, ownership and license are not abided, dispute resolution is not respected and the limitation of liability incurred by the service provider is not traced. From here, it should be noted that the organizations that did not practice risk management faced more problems.

In managing the contract, the organizations suggested two more steps that should be performed

during the contract management phase. The steps are regular implementation meeting and report regularly to steering committee. Regular implementation meeting is necessary to ensure the development of the project is on the right track and complied with the agreed contract. It is also important to report to steering committee so that the stakeholders will always keep abreast with the development of the project.

6.3.4 On-Going Monitoring

An effective monitoring and auditing mechanisms in the outsourcing process should be implemented since written agreement in the contract is not enough [46]. Performing the on-going monitoring phase will enhance the ability to mitigate risks by identifying potential problems before they become catastrophic and thus contribute to success in IT outsourcing.

The on-going monitoring phase takes place when service provider is developing, delivering and maintaining the services or product. During the development phase, it is important for the organization to make sure that the service provider performs accordingly to make sure it can delivers what has been promised. Before the delivery, test should be conducted to make sure that the deliverables are fully functional. The tests include user acceptance test and performance and stressed test. Stressed test allows organizations to know the maximum capability of the products. After the deliverables, it is time for maintenance and support. During maintenance and support, the on-going monitoring should be continuously done. Therefore, any failure can be recovered effectively. Service provider that failed to comply with contract agreement should be punished according to penalty stated in the contract.

All organizations that participated in the survey conducted on-going monitoring to make sure that their service provider will delivered what have been promised. However, performing on-going monitoring is not enough as risk management should be practiced through out all IT outsourcing life cycle. On-going monitoring will not be effective if the organizations skip other phases of risk management. Therefore, even though the organizations performed on-going monitoring, skipping other phases will not make them succeed in this activity. This supports the research done by Grover et al. [61] which mentioned that successful outcomes are unlikely when implementation is poor, regardless of how appropriate a strategic decision may be.

7 Future Research

The results of this study have specific implications for future research. After refinement, a set of questionnaire will be distributed to gather information regarding risk management practices in IT outsourcing. The results of this study can be used to developed risk management in IT outsourcing framework. This framework could assist organizations to manage and reduce risks in IT outsourcing thus increasing the probability of success IT outsourcing projects.

8 Conclusion

The art of delegating IT activities to third party is becoming a trend in many organizations. The involvement of outsider in the project will invite more risks. Those risks will largely impact organization as opposed to the service provider. Therefore, organizations should manage the risk so that the probability of the project to become successful is higher. Research should enhance the effectiveness of risk management to lead to success in IT outsourcing. Therefore, this paper filled in the gap by examining the risk management practices in IT outsourcing project and suggested a conceptual framework that can be used to manage the risk in IT outsourcing projects.

A survey was conducted to validate the conceptual framework. The results of the survey showed that organizations that did not follow the risk management phases closely faced many problems such as late delivery, overrun cost, quality not up to the expectation and many more. Consequently, five out of ten projects surveyed ended with termination clause, a circumstances where the contract was terminated before the completion of the project.

The three organizations that started up with the creation of risk management committee and practiced risk management closely, managed to complete the outsourcing activities successfully. The practices of risk management were still low due to lack of knowledge and skills. Nevertheless, the effort undertaken to practice risk management should be recognized.

From the findings, it has been successfully proven that most of IT outsourcing risks can be controlled and mitigated by applying and practicing risk management. Therefore, risk management in IT outsourcing framework will be developed to assist organizations in managing risks in IT outsourcing projects.

References:

[1] APICS, *Managing the Risks of Outsourcing: A Survey of Current Practices and Their Effectiveness,* 2003.

[2] A.T. Kearney, *A.T. Kearney's 2004 Offshore Location Attractiveness Index: Making Offshore Decisions*, 2004.

[3] A. W. Joshi and R. L. Stump, Determinants of Commitment and Opportunism: Integrating and Extending Insights from Ttransactional Cost Analysis and Relational Exchange Theory, *Revue Canadienne des Sciences de l'Administration*, Vol 16, No. 4, 1999, pp 334.

[4] B. A. Aubert, M. Patry, S. Rivard, and H. Smith, *IT Outsourcing Risk management at British Petroleum,* Cirano (Scientific Series), Canada, 2000.

[5] C. E. Fisher, How to manage Vendor Relationships, *Security Management,* Vol 43, No 8, 1999, pp 123-126.

[6] C. Ramsaran, Outsourcing Obstacle, *Bank System and Technology*, Vol 41, No 6, 2004, p. 38.

[7] C. Saunders, M. Gebelt and Q. Hu, Achieving Success in Information Systems Outsourcing, *California Management Review,* Vol 39, No 2, 1997, pp 63-79.

[8] C. Simmons, Risk Management, 2006. Retrieved at http://sparc.airtime.co.uk//users/wysywig/risk_1.htm on August 15, 2006.

[9] C. Yvonne, "Growing Trend in IT Outsourcing," The Star, Oct. 20, 2003.

[10] Deloitte Consulting White Paper. (2005) Malaysia's edge in the fast evolving outsourcing space. Kuala Lumpur.

[11] Department of Information Resources Texas, Outsourcing Strategies: Guidelines for Evaluating Internal and External Resources for Major Information Technology Projects, Austin, Texas, 1998.

[12] Straub, D. W. & Welke, R. J. (1998). Coping with Systems Risk: Security Planning Models for Management Decision Making. *MIS Quaterly.* 22, 4, pg 441-469.

[13] F. Franceschini, M. Galetto, A. Pignatelli, and M. Varetto, Outsourcing: Guidelines for a Structures Approach, *Benchmarking,* Vol 10, No 3, 2003, pp 246-260.

[14] F. R. Dwyer, P. H. Schurr and Seja Oh, Developing Buyer-Seller Relationship, *Journal of Marketing,* Vol 51, No 2, 1987, p 11.

[15] Federal Financial Institution Examination Council, (FFIEC), *Outsourcing Technology Services*, 2004.

[16] J. Fjermestad, & J. A. Saitta, A Strategic Management Framework for IT Outsourcing: A Review of the Literature and the Development of a Success Factors Model, *Journal of Information Technology Case and Application Research*, Vol 7, No 3, 2005, pp. 42-59.

[17] Funk, J., Sloan, D. & Zaret, S. (2003). Beware the Dangers of Outsourcing. *Optimize.* Pg 68-72.

[18] J. G. Perry, Risk management – An Approach for Project managers, *Project management,* Vol 4, No 4, 1986, pp 211-216.

[19] J. H. Lee, Miranda, S. M. & Kim, Y. M., IT Outsourcing Strategies: Universalistic, Contingency & Configurational Explanations of Success, *Information System Research*, vol. 15, 2004, pp. 110-131.

[20] J. Jorgensen, Managing the Risks of Outsourced IT, *The Internal Auditor,* Vol 53, No 6, 1996, p. 54.

[21] Klosek, J. (2005). Data Privacy & Security are a Significant part of the Outsourcing Equation. *Intellectual Property and Technology law Journal.* 17, 6, pg 15-18.

[22] J. N. Lee, A Strategic Fit Model for IT Outsourcing Success: An Exploratory Approach, presented at Pacific Asia Conference on Information System 2001, 2001.

[23] K. A. Artto, Fifteen Years of Project Management Applications – Where are we Going, in *Managing Risk in Projects,* K. Kahkonen, and K. A. Artto, Eds, London: E & FN Spon, 1997.

[24] K. M. Eisenhardt, Agency Theory: An Assessment and Review, *Academy of Management. The Academy of management Review*, Vol 14, No 1, 1989, p. 57.

[25] KPMG. (2004). *Asia Pacific Outsourcing Survey*. Kuala Lumpur.

[26] KPMG, Strategic Risk Management Survey, Australia, 2005.

[27] L. Poppo and Todd Zenger, Testing Alternative Theories of the Firm: Transaction Cost, Knowledge-based, and Measurement Explanations for Make-or-Buy Decisions in Information Services, *Strategic Management Journal*, Vol 19, No. 9, 1998, p 853.

[28] M. J., Carr, Risk Management may not be for Everyone, *Software Engineering Institute,* Vol 14, No 3, 1997, pp 21-24.

[29] M. J. Earl, The Risks of Outsourcing IT, *Sloan Management Review,* Vol 37, No 3, 1996, pp 26-32.

[30] M. S. Logan, Using Agency Theory to Design Successful Outsourcing Relationship, *International Journal of Logistics Management*, Vol 11, No 2, 2000, p. 21.

[31] MAMPU, The Malaysian Public Sector Information Security Risk Assessment Methodology (MyRAM), Malaysia, 2005.

[32] Gray N. S., PRAM it or Walk Away, *AACE International Transactions,* pp R5-R8, 1998.

[33] NISER, ICT Survey for Malaysia 2001/2002, Kuala Lumpur, 2003.

[34] NIST, Risk Management Guide for Information Technology Systems, USA, 2002.

[35] Noor Habibah Arshad, *An Approach to the Development of Framework for Software Risk Management*, Phd. Dissertation, UKM, 2003.

[36] Noor Habibah Arshad, Azlinah Mohamed, Zaiha Mat Nor, Risk Management Practices in Malaysia's Public Sector, *WSEAS Transaction on Business and Economics Journal,* Vol 3, No 7, 2006, pp 534-54.

[37] Noor Habibah Arshad, Azlinah Mohamed, Zaiha Mat Nor, Risk Factors in Development Projects, in the Proceedings of the 5th WSEAS International Conferences on E-activities, Venice, Italy, Nov 20-22, 2006.

[38] Noor Habibah Arshad, Azlinah Mohamed, Zaiha Mat Nor, The extend of risk management practices in e-government projects, in the Proceedings of the 6th WSEAS International Conferences on Software Engineering, Parallel and Distribution Systems (SEPADS, 07), Corfu Island, Greece, Feb 16-19, 2007.

[39] Noor Habibah Arshad, Yap May Lin, Azlinah Mohamed, Sallehuddin Affandi, *Inherent Risks in ICT Outsourcing Project,* in A. Aggarwal, R. Yager and I. W. Sandberg (Eds.), *Studies in Simulation and Modelling*. Canada, WSEAS Press, 2006.

[40] O. E. Williamson, (1996), *The Mechanism of Governance*, Oxford University press.

[41] P. Cule, R. Schmidt, K. Lyytinen, & M. Keil, (2002). *Strategies for Heading Off IS Project Failure,* in Tinnirello, P. C. (Ed.) (2002), *New Direction in Project Management,* USA: Auerbach Publications.

[42] P. Gottschalk and H. Solli-Seather, Critical Success Factors from IT Outsourcing theories: An Empirical Study, *Industrial Management + Data System*, Vol 105, No 5/6, 2005, p 685.

[43] P. L. Powell, and J. H. Klien, Risk Management for Information System Development, *Journal of Information Technology*, Vol 11, No 4, 1996, pp 309-319.

[44] P. McCormack, The FSA Approach to the Supervision of Outsourcing, *Journal of Financial Regulation and Compliance,* Vol 11, No 2, 2003, pp 113-120.

[45] P. McDougal, Outsourcing's on in a Big Way, *Communication Convergence,* 2003, p17.

[46] Q. Chen, Q. Tu, and B. Lin, Global IT/IS Outsourcing: Expectations, Considerations and Implications, *Advances in Competitiveness Research,* Vol 10, No 1, 2002, p. 100.

[47] R. B. Misra, Global IT Outsourcing: Metrics for Success of all Parties, *Journal of Information Technology Cases and Applications,* Vol 6, No 3, 2004, pp 21-34.

[48] R. G. Kralovets, "A Guide to Successful Outsourcing," *Management Accounting*. Vol 78, No 4, 1996, pp 32-38.

[49] R. Gonzales, J. Gasco, and J. Llopis, Information System Outsourcing Risks: A Study of Large Firms, *Industrial management and Data System,* Vol 105, No 1, 2005, pp 45-62.

[50] R. L. Kliem and. I. S. Ludin, (2002). The Essentials for successful IT Outsourcing in *New Directions in Project management*, P. C. Tinnirello, Ed. New York: Auerbach Publications, 2002.

[51] R. McIvor, A Practical Framework for Understanding the Outsourcing Process, *Supply Chain Management: An International Journal,* Vol 5, No 1, 2000, pp 22-36.

[52] R. N. Charette, The Mechanics of Managing IT Risk, *Journal of Information Technology.* Vol 11, No 4, 1996, p. 374.

[53] S. Dhar and B. Balakrishnan, Risks, Benefits and Challenges in Global IT Outsourcing Perspectives and Practices, *Journal of Global Information Management,* Vol 14, No 3, 2006, pp 39-69.

[54] S. M. Bragg, *Outsourcing* New York: John Wiley & Sons, 1998.

[55] Soon Ang and D. W. Straub, Production and Transaction Economies and IS Outsourcing: A Study of the US Banking Industry, *MIS Quaterly*, Vol 22, No. 4, 1998, p 535.

[56] S. Reed, "Managing Risk in IT Outsourcing," 2005, http://www.alsbridge.com/outsourcing_leadership/nov2005_it_outsourcing.shtml.

[57] Rustagi, S. (2004). Antecedents of success in IS outsourcing: A control theory perspective. (Doctoral dissertation, University of Pittsburgh, 2004).

[58] Syaripah Ruzaini Syed Aris, Noor Habibah Arshad and Azlinah Mohamed, Critical

Review of Risk Management in IT Outsourcing, presented at First Regional Conference on Computational Science and Technologies, Sabah, Malaysia, 29-30 Nov 2007.

[59] Syaripah Ruzaini Syed Aris, Azlinah Mohamed and Noor Habibah Arshad, Preliminary Study on Risk Management in E-Government Outsourcing Projects, in *E-activities: Networking the World, Proceedings of the 6th WSEAS International Conference on e-activities, Puerto De La Cruz, Tenerife, Canary Islands, Spain, 14-16 Dec 2007*, M. Gloria Sanchez-Torrubia, Ed. Canada: WSEAS Press, 2007.

[60] United Nation Division of Public Economics and Public Administration and American Society for Public Administration, *Benchmarking E-Government: A Global Perspective. Assessing the progress of UN Member States*, New York, 2002.

[61] V. Grover, M. J. Cheon and J. T. C. Teng, The Effect of Service Quality and Partnership on the Outsourcing of Information Systems Functions, *Journal of Management Information Systems*, Vol 12, No. 4, 1996, pg 89.

[62] Sullivan, W. E. & Ngwenyama, O. K. (2005). How are Public Sectors Organizations managing IS Outsourcing Risks? An Analysis of Outsourcing Guidelines from three jurisdictions. *The Journal of Computer Information System.* 45, 3, pg 73.