Journal of Media and Information Warfare *Vol. 3, 77-104, 2010*

Conceptual Framework on Information Security Risk Management in Information Technology Outsourcing

Nik Zulkarnaen Khidzir, Noor Habibah Arshad & Azlinah Mohamed
Faculty of Information Technology and
Quantitative Science,
Universiti Teknologi MARA

ABSTRACT

Data security and protection are seriously considered as information security risk for information asset in IT outsourcing (ITO). Therefore, risk management and analysis for security management is an approach to determine which security controls are appropriate and cost effective to be implemented across organization for ITO to secure data/information asset. However, previous established approach does not extensively focus into information security risk in ITO. For that reason, a conceptual framework on information security risk management in IT outsourcing (ISRM-ITO) will be introduced throughout this paper. An extensive amount of literature review on fundamental concepts, theoretical background and previous findings on information security risk management and ITO had been conducted. Throughout the review, theoretical foundation and the process that lead to success in managing information security risk ITO were identified and these findings become a key component in developing the conceptual framework. ISRM-ITO conceptual framework consists of two layers. The first layer concentrates on information security risks identification and analysis before the decision is made to outsource it. The second layer will cover the approach of information security risk management which is used to analyze, mitigate and monitor risks for the rest of the ITO lifecycle. Proposed conceptual framework could improve organization practices in information security study for IT outsourcing through the adoption of risk management approach. Finally, an approach to determine a cost effective security control for information security risk can be implemented successfully in the ITO cycle.

ISSN 1675-1302

Keywords: *Risk Management, Information Security, IT Outsourcing, Conceptual Framework, Risk Mitigation*

Introduction

Outsourcing is an effective way to cut cost, launch new business ventures and improve efficiency. Outsourcing is one of the ways for the government to operate more effectively while saving money (McDougal, 2003). In a recent research conducted by Information Week Research (Engardio and Kripalani, 2006), 65% of the respondents realize that outsourcing offers cost savings and another 50% believes that it provides high-skill vendor's operational expertise. Other benefits of outsourcing include cost restructuring, quality improvement, knowledge (Engardio and Kripalani, 2006), contract, and improved method of capacity management of services and technology where the risk of providing the access capacity is borne by supplier or vendor. Currently, Malaysian government sector actively outsource ICT project and services. Systems or processes most commonly outsourced namely are ISP services, web hosting, ICT application maintenance and support, ICT infrastructure, programming, e-business solution, application analysis, application services provision, support end user, staff/user training, ICT security audit and security policy or standards development (NISER, 2003; Noor Habibah, Yap, Azlinah and Sallehidding, 2007).

Even though the ITO approaches provide many advantages to businesses, it still entails some risks (Aubert, Patry and Rivard, 2005). Top 10 ICT outsourcing risk ranked based on importance are Cost-Reduction Expectations, Data Security/Protection; Process Discipline such Capability Maturity Model (CMM), Lost of Business Knowledge, Vendor Failure to deliver, Scope Creep, Culture, Turnover of Key Personnel, and Knowledge Transfer (Davison, 2003).

Therefore, it is essential for an organization to maintain the best condition of information security posture to ensure the ITO process is less interrupted by information security risk. In order to do that, information security risk management approach is required to provide better execution of information security management plan. However, previous studies on information security risk management has not seriously considered ITO (Alberts and Dorofee, 2002; Stolen et al., 2003; International Security Technology Inc., 2000; Suh and Han, 2003). Currently not many researchers highlighted on how to manage information security risk in

ITO lifecycle. Thus, this research focuses on contribution of information security risk management to the success of an ITO implementation.

This paper explores the adoptions of information security risk management perspective into ITO lifecycle and proposing a conceptual framework based on extensive theoretical works. This paper focuses on the second most critical risk in ICT outsourcing which is data security/ protection.

Related Work

Extensive review on related work in ICT outsourcing, information security domains, and fundamental concept of risk management as well as information security risk management provide a landscape for the study to identify a knowledge gap in the field. Literature review on information security risk in ICT outsourcing was also synthesized in a structured manner.

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, who develop, manage and administer these activities in accordance with agreed upon deliverables, performance standard and outputs, as set forth in contractual agreement (Dhar and Balakrishnan, 2006).

Besides the advantages of ICT outsourcing approach in improving processes and services, they still come together with potential risks that could emerge during ICT outsourcing cycle. Recent study discovered 10 risks in outsourcing the needs to be successfully addressed to ensure the objective of outsourcing is achieved. According to the study, the second highest risk with outsourcing is data/ information security and protection (Davison, 2003). This is another critical risk that IT organizations need to evaluate in any kind of outsourcing to be able to successfully deal with. Before deciding on an outsourcing supplier, be sure to check if they have sufficient robust security practices and if they can meet the security requirements they have internally. While most IT organizations find vendor security practices impressive, for example the risk of security breaks or intellectual property protection is inherently raised when working in international business; privacy concerns must also be completely addressed to minimize negative impact to organization.

Therefore, the conceptual framework should address data/ information security risk by providing an appropriate risk management approach for better security and protection management plan in ITO cycle.

Information Security Domains

Information security is an organisation’s approach to maintaining confidentiality, availability, integrity, non-repudiation, accountability, authenticity and reliability of its IT systems (Anita & Labuschagne, 2005). Information security is required because the technology applied to information creates risks. Generally, information might be improperly disclosed (its confidentiality could be exposed), modified in an inappropriate way (its integrity could be jeopardized), or destroyed or lost (its availability could be threatened) (Blakley, McDermott & Geer, 2001).

The ISC Common body of knowledge (CBK) is a global organization and a collection of topics that is relevant to information security where professionals highlight security management as one of the ten domains relevant to information security’s body of knowledge (Merkow & Breithaupt, 2005; Tipton & Krause, 2008). The domain emphasizes the importance of comprehensive security plan that includes security policies and procedures for protecting data and its administration. There are 10 domains in information security (MAMPU, 2005b; Merkow & Breithaupt, 2005; Davison, 2003; Tipton & Krause, 2008) which includes Security policy, Organizational security, Personal Security, Access Control, Compliance, Business Continuity, System Development & Maintenance, Communication & Operation Management, Asset Classification & Control, and Physical Environmental Security as shown in Figure 1. However, for the purpose of this research, the focus is on the five related information security domains consisting of Physical & Environmental Security, Asset Classification & Control, System Development & Maintenance, Organizational Security, and Access Control.

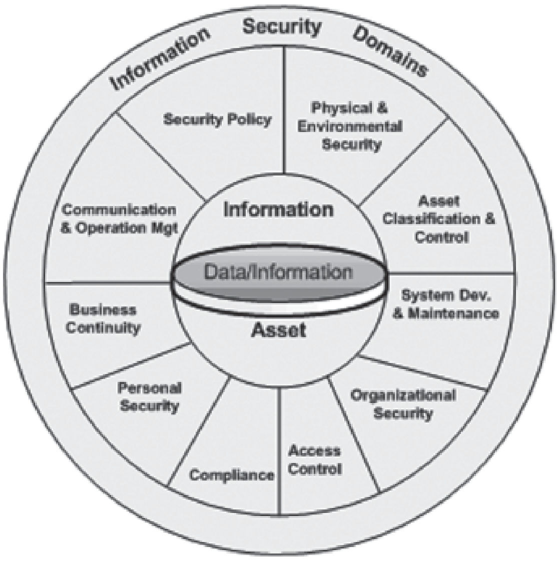
Information Security Domains
Security Policy
Physical & Environmental Security
Asset Classification & Control
System Dev. & Maintenance
Organizational Security
Access Control
Compliance
Personal Security
Business Continuity
Communication & Operation Mgt
Information
Data/Information
Asset

Figure 1: Information Security Domains

Risk Management

Risk and risk management have been studied in a variety of fields, such as Insurance, Economics, Management, Medicine, Operations Research, and Engineering (Aubert et al., 2005). Each field addresses risk in a fashion relevant to its object of analysis, hence, adopts a particular perspective. Basically, risk management is activity directed towards the assessing, mitigating and monitoring of risks. The reviews concentrate into main conceptualization of risk and risk management found in various fields. Multiple perspectives will be adopted from the review which is relevant to our study on information security risk in ITO. These perspectives are summarized in Table 1.

Information Security Risk Management

At present, there are numerous risk analysis methodologies available where some of which are qualitative while others are more quantitative in nature. However, these methodologies have a common goal of estimating the overall risk value. Risk analysis methodology such OCTAVE (Alberts and Dorofee, 2002) and CORAS (Stolen et al., 2003)

Table 1: Multiple Risk Perspectives

Risk Perspectives	Description	Ref
Risk as an Undesirable Event	Risks are the multiple undesirable events that may occur in organization. This perspective are widely use in many field of studies	Aubert et al. (2005); Levin and Schneider (1997)
Risk as a Probability Function	Insurance adopts this perspective and uses mortality tables to estimate probabilities. In this context, a “good risk” will be a person with a low probability of dying within a given period (and hence, for the insurance company, a low probability of having to pay a compensation) and a “bad risk” would be a person with a high probability of dying within the period.	Aubert et al. (2005)
Risk as Variance	Finance adopts a different perspective of risk, where risk is equated to the variance of the distribution of outcomes. The extent of the variability in results (whether positive or negative) is the measure of risk. Risk management means arbitrating between risk and returns.	Aubert et al. (2005); Schirripa and Tecotzky (2000)
Risk as Expected Loss	Car insurance, adopt a perspective of risk as expected loss. They define risk as the product of two functions: a loss function and a probability function.	Aubert et al. (2005)

provide a qualitative information security risk analysis for information communication technology. Three examples of quantitative methodologies are Information Security Risk Analysis Methodology (ISRAM) (Karabacak and Sogukpinar, 2005), Cost-of Risk Analysis (CORA) (International Security Technology Inc, 2000), Information System (IS) analysis based on a business model (Suh and Han, 2003), Malaysian Government Risk Assessment Methodology (MyRAM) (MAMPU, 2005b) and Malaysian Public Sector Information Security High-Level Risk (MAMPU, 2005a).

From the review of these approaches highlight the inflexibility of methodologies, models or its components for ITO environment. Moreover, they are not specifically developed to assess, analyze and mitigate an information security risk in ITO. OCTAVE approach concentrates on assets, threats and vulnerabilities. Even though OCTAVE remains a compelling framework for detailed investigation into many aspects of risk management and best practices on all security issues, its approach is not extensively focused into information security risk for ITO (Alberts and Dorofee, 2002). CORAS approach introduce an integrated risk management and system development process as one of the pillars where focus lies on the tight integration of viewpoint-oriented UML-like modelling in risk management process. CORAS (Stolen et al., 2003) approach of risk management is sometimes difficult to implement because its requirement specification may change during the system development process thus causing the information security risk to change. Unlike other risk management approach, Information System Risk Assessment Model (ISRAM) (Karabacak and Sogukpinar, 2005), is a survey-based model applying a quantitative approach to risk analysis that allows for participation of the manager and staff of the organization but does not use techniques such as Single Occurrence Losses (SOL) or Annual Loss Expectancy (ALE). In ITO, quantitative risk assessment approach is still required to assess and analyze the probability of information security risk on information system. Qualitative analysis sometimes does not always provide adequate information to make a decision on a mitigation plan. Although Business Model-Based Information System Risk Analysis fixes some limitation on previous risk analysis approach by measuring asset's value, replacement cost and tangible asset's value from the perspective of operational continuity (Suh and Han, 2003), it still doesn't measure intangible asset for instance corporate intellectual property. Furthermore, unauthorized exploitation of intellectual property (Hinson, 2008, pp. 2) is one of the critical information security risks that usually occur in ITO which needs appropriate control in order to reduce the impact to the organization. MyRAM (MAMPU, 2005b) and HiLRA (MAMPU, 2005a) are two information security risk management approaches developed for the Malaysian government public sector. HiLRA (MAMPU, 2005a) provides a guide in implementing high-level information security risk assessment to obtain an early view of the risk level in the agency. Detail assessment is conducted by applying MyRAM (MAMPU, 2005b) approach. However both of these approaches are not extensively focus into information security risk in ITO cycle. The summarization of these approaches is as shown in Table 2.

Information Security Risk in IT Outsourcing

Risk Survey in 2000 by Deloitte Touche Tohmatsu identified information security risk as one of the major key risk area in ITO project (Tohmatsu, 2000). Information security risk is possibilities of threats on vulnerabilities that may because impacts contributed to information security incidents (Hinson, 2008, pp. 5). Some examples are theft of personal data, information leakage, extraction or loss and unauthorized exploitation of intellectual properties. These risks are caused by lack of control on threats and vulnerabilities. Threats (e.g. Fraudster/ Hackers, organized crime, unauthorized access, malware authors, etc) are actors or situation that might deliberately or accidently exploit vulnerabilities causing information security risk (Hinson, 2008, pp. 2). Vulnerabilities (e.g. Software bugs, poor/ missing governance of information assets, etc) are the flaws or weaknesses in system security procedure, design, implementation or internal control that could be exploited resulting in security breach, violation of system security policy and other impacts (Hinson, 2008, pp. 5; Hinson, 2008, pp. 2). Table 3 shows some of the information security risk related to ITO lifecycle.

Table 2: Information Security Risk Management Approach

Related Risk Management Approach	Description	Ref
OCTAVE	Approach concentrates on assets, threats and vulnerabilities.	Alberts and Dorofee (2002)
CORAS	Integration of risk management and system development process as one of the pillars to focus lies on the tight integration of viewpoint-oriented UML-like modelling in risk management process.	Stolen et al. (2003)
Information Security Risk Analysis Methodology (ISRAM)	Survey-based model applying a quantitative approach to risk analysis that allows for participation of the manager and staff of the organization but does not use techniques such as Single Occurrence Losses (SOL) or Annual Loss Expectancy (ALE).	Karabacak and Sogukpinar (2005)
Cost-of Risk Analysis (CORA)	Risk Model uses data collected about threats, function and assets, and vulnerabilities of the functions and assets to the threats to calculate the consequences, which are the losses due to the occurrences of the threats.	International Security Technology Inc (2000)
Information System (IS) analysis based on a business model	Define asset's value and then not only bases the analysis on its replacement cost, but also measures the tangible asset's value from the viewpoint of operational continuity.	Suh and Han (2003)

(*Continued*)

(*Table 2 - Continue*)

MyRAM (Organization/ Nation)	Malaysian Government Risk Assessment Methodology (MyRAM) Identification of ICT: • Assets • Vulnerabilities • Threats • Associated Risk • Safeguards for the identified assets.	MAMPU (2005b); MAMPU (2002)
HiLRA (Organization/ Nation)	Malaysian Public Sector Information Security High-Level Risk Assessment.	MAMPU (2005a); MAMPU (2002)

An effective protection and security control will contribute to the success of ITO. Thus, this paper presents a conceptual framework to manage information security risk in ITO as part of the key element in developing an information security management plan.

Table 3: Information Security Risk in IT Outsourcing

ITO Lifecycle	Information Security Risk	Ref
Analysis of decision to outsource	Information Leakage, Poor Information Security Study	Hinson (2008) pp. 5; Garfinkel (2007); Merkow and Breithaupt (2005)
Selection of the service provider	Unauthorized Exploitation of Intellectual Property Right (IPR)	Hinson (2008) pp. 5; Ju, Kim and Kim (2007); Sota (2004); Vassiliadis, Fotopoulos, Ilias and Skedras (2005)
Contract Management	Information Leakage	Hinson (2008) pp. 5, Garfinkel (2007)
On-Going Monitoring	Environmental Disaster, Information Leakage	Hinson (2008) pp. 5, Halliday, Badenhorst, and Von Solms (1996), Bitha and Von Solms (2004), Hawkins, Yen and Chou (2000)

This framework would be a dedicated framework for information security risk in ITO outsourcing cycle in order to cater most of the information security risks in ITO. The framework will ensure better handling of information security risk and ensure the confidentiality of data in most of their ITO cycle. The proposed conceptual framework will introduce recommendations and steps to manage information security risk that may occur during ITO cycle as part of the security guarantee to outsource IT projects. Eventually, this will ensure that risks on information confidentiality, integrity and availability in ITO project implementations are controlled and manageable.

Methodology

An extensive amount of literature review on fundamental concepts, theoretical background and previous findings on information security risk management and ITO has been conducted. Throughout the review, the best practices that lead to success in managing information security risk in ITO are identified. Then, the identified practices become a key component to develop the conceptual framework.

Conceptual Framework for ISRM-ITO

Risk management is a well-established practice in a variety of fields. There are many researchers who introduced numerous risk management approaches to understand associated risk to prepare their security management plan better (Alberts and Dorofee, 2002; International Security Technology Inc., 2000; Karabacak & Sogukpinar, 2005; Stolen et al., 2003; Suh and Han, 2003). However, most of them failed to specifically manage information security risk in ITO. Furthermore, most of them concentrated on project risk management (Syaripah Ruzaini, Noor Habibah and Azlinah, 2008) in ITO but not the information security risks. Therefore, this paper proposes a conceptual framework to manage information security risk in ITO. The framework is divided into two levels as shown in Figure 2. The first level discusses on the phases in Information Security Risk Management (ISRM) while the second level is on the ITO approach. The approach takes into consideration the questions that arise in ITO which have been answered by supporting theories and the integration process of information security risk management.

Consequently, the approach is then enhanced by the addition of information security risk management fundamental principle which is a key element that should be conducted at each and every phase in the approach. As a result, possible risks that might emerge in each approach can be identified and managed.

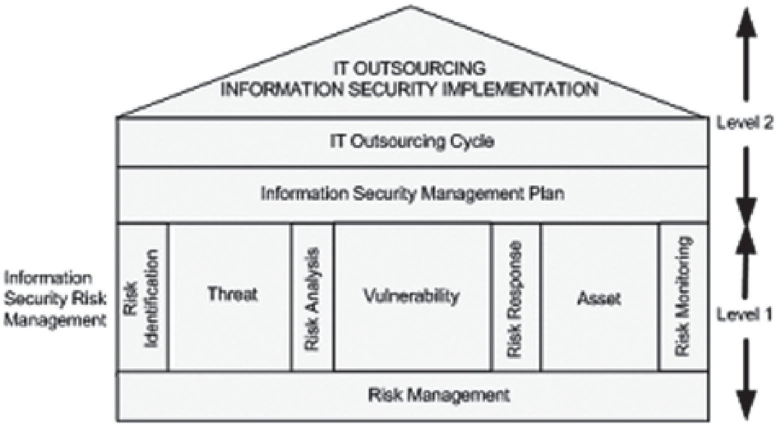

Figure 2: Conceptual Framework of Information Security Risk Management (ISRM) for IT Outsourcing

Risk Management

Risk management is an activity directed towards the assessing, mitigating and monitoring of risks. The aim of Risk Management is to identify measures and control uncertain events, in order to minimize loss, and optimize the return of the money invested for security purposes. As shown in Figure 2, the conceptual framework is based on the core principle of risk management as a primary foundation. In businesses, risk management entails organized activities to manage uncertainty and threats and requires people to follow procedures and use tools in order to ensure conformance with risk-management policies.

In information security, identifying the most critical assets through the analysis of threats and assessment of vulnerabilities to determine the risk (i.e. the expected consequences of specific types of attacks on specific assets) is important. People need to identify ways or options to reduce these risks as a treatment to the risk and finally prioritize risk reduction measures through appropriate strategies. The strategies include transferring the risk to another party, avoiding the risk, reducing the negative effect of the risk, and accepting some or all of the consequences of a particular risk.

However, the conceptual framework will adopt the core principle of risk management for information security in ITO lifecycle.

Information Security Risk Management

Information Security Risk Management is a concept whereby a systematic approach in assessing information security risks and developing an appropriate protection strategy is a major component of an effective information security program (Alberts and Dorofee, 2002). This fundamental principle is an overlapping step that should be performed at each and every approach of managing information security risk in ITO. Every step has its own key elements in order to achieve the objective and is deliverable at each phase.

The primary step in risk management is risk identification. It involves identifying specific elements of the three components of risk; asset, threats and vulnerabilities (MAMPU, 2005b; Miller & Gregory, 2008). Identifying an organization's asset and determining their value is a critical step in determining the appropriate level of security. This conceptual framework will adopt a qualitative and quantitative asset valuation method which is relevant. The second step in risk management is risk analysis. A risk analysis brings together all elements of risk management (identification, analysis, response and monitoring) and is critical to an organization in developing an effective risk management strategy (Miller and Gregory, 2008, pp. 141). The third step in information security risk management is risk response. A properly conducted risk analysis provides the basis for selecting appropriate safeguards and countermeasure (Miller and Gregory, 2008, pp. 144). A safeguard is a control or countermeasure that reduces risk associated with a specific threat. The absence of a safeguard against a threat creates vulnerability and increases the risk.

Development of the conceptual framework is based on related work and theoretical foundation in information security risk management and ITO. The theoretical foundation and process of information security risk management has been supported by other researchers in their risk management approach. Risk management phases of the conceptual framework and supported theoretical foundations are described in Table 4. Each of the information security risk management approach has its own set of steps in order to achieve the objectives of each phase. The steps for each approach are as discussed in Table 4.

Table 4: Information Security Risk Management Phases

Information Security Risk Management Approach	Description	Ref
Risk Identification	A process of identifying the risk to the system security	MAMPU (2005b); Miller & Gregory (2008); Appin Security Group (2009)
Risk Analysis	A process of determining the probability of occurrences, the resulting impact, and additional safeguard that would mitigate impact	Alberts and Dorofee (2002); Chen (2006); Dhar and Balakrishnan (2006); Bitha and Von Solms (2004); MAMPU (2005b); Vorster and Labuschagne (2005); Wawrzyniak (2006); Stoneburner, Goguen and Frenga (2006); Miller and Gregory (2008) pp. 141
Risk Response/ Treatment	Countermeasure that reduces risk associated with a specific threats (risk reduction, assignment/transference, avoidance or acceptance)	Bitha and Von Solms (2004); Miller and Gregory (2008) pp. 144
Risk Monitoring/ Reporting	Maintenance of records of incidents; Identifying new risk and determining if any of the known risks have changed; control & countermeasure effectiveness; compliance with standards/regulation; providing vulnerability and incident alerts; maintaining the risk management plan.	Bitha and Von Solms (2004); MAMPU (2005b)

Risk Identification

Identification of risk involves Asset Valuation, Threats Analysis and Vulnerability Assessment. The basic elements in determining the value of an asset are initial and maintenance cost, organizational value and public value. Asset valuation facilitates cost benefit analysis and supports management decisions regarding selection of appropriate safeguards. It can also be used to determine insurance requirement, budgeting and replacement cost. Identification of information security risk is critical in ITO cycle especially in analyzing the decision to outsource. Identification of risks are based on asset valuation, threats analysis and vulnerability assessment within the scope of ITO project. Therefore, identification of risk in terms of asset value, vulnerabilities and threats related to data/information are to be seriously considered during the analysis of decision to outsource. During the phase of selecting a service provider, identification of risks can be done by reviewing the technical and financial proposal provided by the service provider.

Risk Analysis

There are four steps involved in information security risk analysis. These steps include (1) identifying the assets to be protected, including their relative value, sensibility or importance to the organization through asset valuation; (2) Defining specific threats, including threats frequency and impact data by conducting threats analysis; (3) Calculating Annualized Loss Expectancy (ALE) for the risk. ALE provides a standard, quantifiable measure of the impact that a realized threat has on an organization's assets. Therefore, ALE is particularly useful to determine the cost-benefit ratio of a safeguard or control. Finally, (4) selecting appropriate safeguards based on risk identification through vulnerability assessment and risk control. Table 5 describes the variables required to estimate the annual loss for the threats or event.

Table 5: Variables to Calculate Annualize Loss Expectancy

Variables	Description	Ref
Annualized Loss Expectancy (ALE)	Single Loss Expectancy X Annualized Rate of Concurrency	Miller and Gregory (2008) pp. 141; Miller and Gregory (2008) pp. 144
Single Loss Expectancy (SLE)	Measure of the loss incurred from a single realized threat or event, expressed in monetary value. It is calculated as Asset Value ($) x Exposure Factor (EF)	Miller and Gregory (2008) pp. 144
Exposure Factor (EF)	Measure of the negative effect or impact that a realized threat or event would have in a specific asset, expressed as percentage (%)	Miller and Gregory (2008) pp. 144
Annualized Rate of Occurrence (ARO)	Estimated annual frequency of occurrence for the threat or event	Miller and Gregory (2008) pp. 144

In ITO, we identify the assets to be protected either it is the organization's or the service provider's assets. Analysis of threats and vulnerabilities also need to be conducted by the organization and outsource parties as specified in the ITO contract. Calculation of the ALE for the risks is useful to determine the cost-benefit ratio of a safeguard or control provided by the service provider. Therefore, this cost-benefit ratio of a safeguard will be part of the consideration factor during selection of service provider in an ITO cycle.

Risk Response/Treatment

Risk response or countermeasure is considered as a treatment to reduce risks associated with a specific threat. Risk response includes risk reduction, risk assignment, risk acceptance and risk avoidance. Risk response/ treatment may be a combination of technical and non-technical changes (Stoneburner et al., 2006; Bitha and Von Solms, 2004; Gordon, Loeb & Sohail, 2003; MAMPU, 2005b; Chen, 2006; Vorster and Labuschagne, 2005) Technical changes involve security equipment (e.g., access controls, cryptography, firewalls, intrusion detection systems, physical security, antivirus software, audit trails, backups) and management of that equipment. Non-technical changes could include policy changes, user training, and security awareness. Risk Reduction by implementing the necessary security controls, policies, and procedures to protect an asset can be achieved by altering, reducing, or eliminating the threats or vulnerability associated with the risks. Risk assignment can be done through transferring the potential loss associated with the risk to a third party, such as an insurance company. Another option of risk treatment is risk acceptance. This is sometimes done for convenience but is more suitable when the cost of other countermeasure is prohibitive and potential risk probability is low. Conversely, if the analysis shows that the risk is too high, treatment of such avoidance is the best option so that the impact to the organization can also be reduced or eliminated.

However, risk responses in ITO depend on risk types and phases involve in the cycle. For example, if the information security risk is found to be too high during an analysis of decision to outsource, then, treatment of such avoidance is the best option. As a result, that particular ITO project will not be approved.

Risk Monitoring/ Reporting

The monitoring of risk is normally conducted by the internal resources of an organization (Bitha & Von Solms, 2004; MAMPU, 2005b). Nevertheless, in ITO, both parties (internal and outsource parties) are responsible in monitoring the risks as clearly defined in the contract document. For example, internal resources are responsible in determining the controls and the effectiveness of the countermeasures being used. Meanwhile, outsource parties maintain records of incidents involving the information security risk. However, scope of risk monitoring depends on types and budgets allocated for an ITO project. Effective reporting is an essential mechanism of risk management. Hence, reports must be written in a form which is understandable across organizational level from technical staff to senior management as well as outsource parties. As a result, communication errors among them can be reduced so that inputs for decision making are more accurate and sufficient.

Threats, Vulnerabilities and Assets

Beyond basic security fundamentals principle, the concepts of risk management are the most important and complex part of the information security and risk management domains. Risk management in information security primarily concerns threats and vulnerabilities of assets. Threats refer to any natural or man-made circumstance or event that could have an adverse or undesirable impact, minor or major, on organizational asset (Hinson, 2008, pp. 2; Miller and Gregory, 2008). Vulnerability refers to the absence or weaknesses of a safeguard in an asset that makes a potential threat more harmful or costly and more likely to occur, or it might occur more frequently (Hinson, 2008) pp. 2; Miller and Gregory, 2008). In propose conceptual framework, an asset could be a resource, process, product, or system that has some value to an organization and must therefore be protected (Miller and Gregory, 2008, pp. 139). Threats and vulnerabilities are much greater in ITO because service providers might not expose the vulnerabilities of their services that could contribute to information security incidents. Assets may be tangible such as computers, data, software and records; or intangible such as privacy, access, public image and ethics; and may likewise have a tangible value (purchase price) or intangible value (competitive advantage). However, the conceptual framework concentrates on data/ information as the asset group including documented (paper or electronic) information or intellectual information which is used to meet the missions and/or objectives of the information (MAMPU, 2005b). Table 6 shows vulnerabilities, threats and information assets as very important aspects to consider when dealing with information security.

Table 6: Information Security Concerns of Vulnerabilities, Treats and Assets

Information Security key concerns	Description	Ref
Treats	Any natural or man-made circumstance or event that could have an adverse or undesirable impact, minor or major, on organizational asset	Hinson (2008) pp. 2; Miller and Gregory (2008) pp. 139; Kaplan (2005)
Vulnerabilities	Absence or weaknesses of a safeguard in an asset that make a threat potential more harmful (can be exploited) or costly, more likely occur, or likely to occur more frequently.	Hinson (2008) pp. 2; Miller and Gregory (2008) pp. 139; Kaplan (2005)
Assets	Identifying and organization's assets and determining their value is a critical step in determining the appropriate level of security.	Miller and Gregory (2008) pp. 141

Information Security Management Plan

Risk management standards for information security have been developed and published as part of ISO/IEC 27000 Series. Recently, ISO/IEC 27005 has been published in June 2008 to provide techniques for information security risk management that includes information and communication technology security risk management (Hinson, 2008, pp. 5). The standards support the general concepts specified in ISO/IEC 27001 and are designed to assist the satisfactory implementation of information security based on a risk management approach. Knowledge of the concepts, models, processes and terminologies described in ISO/IEC 27001 and ISO/IEC 27002 is important for a complete understanding of ISO/IEC 27005:2008 (MAMPU, 2005b). The standards set up a key point of reference for researchers and other information security professionals to develop or formulate a variety of risk assessment and analysis methodology as well as framework to secure information assets through risk management approaches. It is applicable to all types of organizations (e.g. commercial enterprises, government agencies, non-profit organizations) which intend to manage risk that could compromise the organization's information security (International Organization for Standardization, 2008).

Risk management and analysis of security management are approaches to determine which security controls are appropriate and cost effective to be implemented in certain environment and organization (Merkow and Breithaupt, 2005). ISO/IEC 27001 is a globally acknowledged standard defining the requirements for an Information Security Management System (ISMS). The standard considers Information Security as a combination of people, process, and technology (Appin Security Group, 2009). An Information Security Management plan is part of the ISMS and it includes all of the elements that organizations use to manage and control their information security risks. Risk management approaches contribute to the development of information security plan by identifying and analysing potential information security risks as well as how to plan an appropriate control or countermeasure to mitigate the risks. Basically the concept provided in the standards emphasizes on risk management approaches for information security. Organization management strategy to secure information asset will be defined in detail in the information security management programme or plan. However, the conceptual framework will use the MS ISO 17799 standard because it was developed based on Malaysia's perspective. In most current practices, risk management approach to identify and analyze information security risk factor is the key component in security management plan. Related standards and guidelines for information security risk management are shown in Table 7.

IT Outsourcing Cycle

IT Outsourcing lifecycle consists of four main phases (Syaripah Ruzaini et al., 2008).The first phase is analysis of decision to outsource. In ITO, this step concerns the decision whether to outsource or not after considering the information security risk possibilities. Risk identification and analysis on threat, vulnerability and asset should be conducted in order to determine information asset value and to identify possible consequences of threat and vulnerability. The second phase is selection of a service provider. It is important to select a service provider that is more concerned over information security risks. Therefore, they are able to provide a secure ITO environment to their clients.

Table 7: Information Security Management Standards & Guidelines

Information Security Management Standards/Guidelines	Description	Ref
ISO 27001 (Global Standard)	Information Security as a combination of people, process, and technology	MAMPU (2005b); Appin Security Group (2009)
ISO/IEC 13335-1 GMITS (Global Standard)	Part 1: Concepts and models for information and communications technology security management (Descriptions of the major security elements and their relationships that are involved in ICT security management) Current revised title is BS ISO/IEC 13335-1:2004	MAMPU (2005b); Appin Security Group (2009)
ISO/IEC 13335-2 GMITS (Global Standard)	Part 2: Information security risk management (Standards origin from Switzerland currently widely used) Current revised title is ISO/IEC 27005:200	MAMPU (2005b)
ISO/IEC 13335-3 GMITS (Global Standard)	Guidelines of the Management of IT Security Part 3: Techniques for the management of IT Security	MAMPU (2005b)
ISO/IEC 13335-4 GMITS (Global Standard)	Guidelines for the management of IT Security Part 4: Selection of safeguards Current revised title is ISO/IEC 13335-4:2000	MAMPU (2005b)
ISO/IEC 13335-5 GMITS (Global Standard)	Guidelines for the management of IT Security Part 5: Management Guidance on Network Security Current revised title is ISO/IEC TR 13335-5:2001	MAMPU (2005b)
ISO/IEC 14516 (Global Standard)	Guidelines for the Management of Trusted Third Parties Services Current revised title is ISO/IEC TR 14516:2002	MAMPU (2005b)
BS 7799 (ISO/IEC 17799:2000) – Organization/Nation	Information Technology. Security Technique. Code of Practices for Information Security Management (Origin British Standards – BS 7799) Current revised title is ISO/IEC 17799:2000 Malaysia Standards – MS ISO 17799	MAMPU (2005b); Appin Security Group (2009)

(*Continued*)

(*Table 7 - Continue*)

MyMIS (Organization/ Nation)	Malaysian Public Sector Management of Information and Communication Technology Security Handbook – Based on NIST Handbook (US)	MAMPU (2005b); MAMPU (2002)
ISO/IEC 15947 (Domain Specific)	IT intrusion detection framework. (Computer technology, Data security, Data storage protection, Safety measures, Data processing, Information exchange, Data transmission, Risk assessment) - Current revised title is ISO/IEC TR 15947:2002	MAMPU (2005b)
ISO/TR 13569 (Domain Specific)	Information technology. Security techniques. Information security programme for Financial services industry. (Policies, organization and the structural, legal and regulatory components, Selection and implementation of security controls, Elements required to manage information security risk) Current revised title is ISO/TR 13569:2005	MAMPU (2005b)
IETF RFC 2196 (Domain Specific)	Site/Web Security Handbook • Guide to developing computer security policies and procedures for sites that have systems on the Internet. • Provide practical guidance to administrators trying to secure their information and services. • Web Security Risk Assessment/Analysis	MAMPU (2005b)

Contract management is the phase where an organization should design and manage the contract for the ITO project secure environment. An ITO contract should clearly states the method of protection of information asset during the project lifecycle. The purpose of on-going monitoring is to have better control from information security risk and maintain the security of information asset in the organization. An organization should monitor the service provider’s activities to ensure a secure ITO environment during project implementation.

Consideration of information security risk management in these four phases of an ITO cycle is relevant because the validation of the cycle has been confirmed by previous studies done in Malaysia (Syaripah Ruzaini et al., 2008). Therefore it is also significant to our study towards the development of an ITO information security implementation environment. Table 8 summarizes some of the literature review related to information security issues in ITO.

Table 8: Information Security Issues in IT Outsourcing

IT Outsourcing	Description	Ref
Associated Risk	The risk associated to an ICT outsourcing project must be evaluated and managed.	Engardio and Kripalani (2006)
Strategy/Approach	While it can bring several benefit, ICT outsourcing entails some risk	Aubert et al. (2005)
Security Risk Survey	Risk Survey 2000 has identified information security is one of the major key risk areas	Engardio and Kripalani (2006); Tohmatsu (2000)
Data Security & protection	Data Security and protection is one of the ICT outsourcing risk	Davison (2003)

IT Outsourcing Information Security Implementation

A comprehensive and dedicated risk management approach should be fully engaged in every phases of an ITO cycle. Before implementation, establishment of teams responsible to the tasks conducted in each phases of ITO is required. Risk management team is responsible in conducting the identification and analysis of risks associated in an ITO cycle. Basically, the team will be responsible in identifying the risk rating, propose best practices safeguard rating, and risk level rating. By adopting the information security risk management's (ISRM) approach to an ITO cycle, the conceptual framework introduces two major phases in ITO with different key elements of risk management steps in each phase. The phases are categorized into Pre-ITO and During-ITO. ITO information security implementation will be discussed in the following section. Figure 3 shows the implementation of information security in ITO.

Pre-IT Outsourcing Phase

Pre-ITO phase involves identification and analysis of information security risk for data/information assets in organization. Information security risks identification and analysis are required during analysis of decision to outsource, selection of service provider and contract management stage in IT outsourcing cycle. Service provider's practices of security and

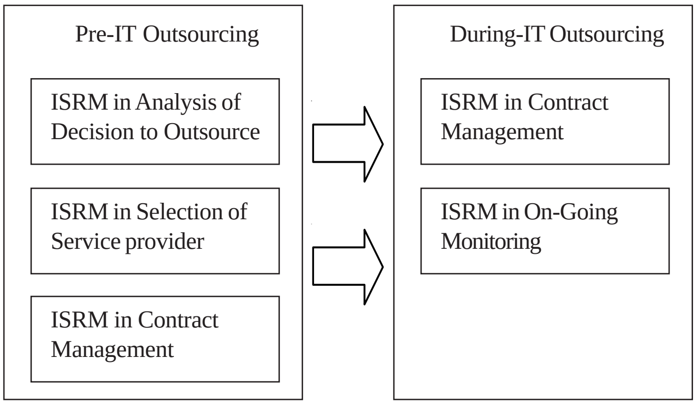
Pre-IT Outsourcing
ISRM in Analysis of Decision to Outsource
ISRM in Selection of Service provider
ISRM in Contract Management
During-IT Outsourcing
ISRM in Contract Management
ISRM in On-Going Monitoring

Figure 3: ITO Information Security Implementation

responsibility towards disaster recovery plan are the elements to consider in the process of identifying and analyzing information security risks in the phase of selecting a service provider. During these phases, risks response and monitoring are not compulsory if an organization decides not to outsource the IT project due to the unacceptable or high level information security risks. Information security risk level is determined based on the risk level rating table as shown in Table 9.

Table 9: Risk Level Rating

Risk Level	Description
3 : High Risk	Lack of safeguard/control. The organization’s data/information asset is at High Risk.
2 : Medium Risk	Available safeguard/controls could be added to or improved. The organization’s data/information asset is at High Risk.
1 : Low Risk	Risk vs. safeguards/controls in place almost meet the organization’s operational requirement. The organization’s data/information asset is at Low Risk.
0 : Negligible Risk	Risks vs. safeguards/controls in place are sufficient or just nice. The organization’s data/information asset has Negligible Risk.
-1 : Negligible Risk (Slightly Overprotected)	Risks vs. controls in place are not cost effective. There are slightly more safeguards/controls. The organization’s risk is still negligible as well as slightly overprotected.
-2 : Negligible Risk (Moderately Overprotected)	Risks vs. controls in place are not very cost effective. There are slightly more safeguards/controls. The organization’s risk is still negligible as well as moderately overprotected.
-3 : Negligible Risk (Extremely Overprotected)	Risks vs. controls in place are extremely not cost effective. There are slightly more safeguards/controls. The organization’s risk is still negligible as well as extremely overprotected.

Safeguard rating in IT outsourcing phases must also be considered when determining risk level rating (MAMPU, 2005a). Table 10 describes the best practise safeguard rating used in proposed conceptual framework.

Table 10: Best Practices Safeguard Rating

Best Practises Safeguard Rating	Description
0 : Sufficient (Should be Improved)	The derived number of safeguards to be implemented which is sufficient for organization's information security risks control
-1 : Low	The least amount of safeguards/controls to be implemented
-2 : Medium	An average amount of safeguards/controls to be implemented
-3 : High	A majority amount of safeguards/controls to be implemented

During-IT Outsourcing Phase

ISRM approach in During-ITO phase involves identification, analysis, response and monitoring of information security risk on data/information asset in an organization during the contract management and On-Going Monitoring stage. During-ITO phase refers to the period of the IT outsourcing project contracted to the selected service provider. Within this period, the complete cycle of ISRM approach is compulsory in order to design an appropriate security risk management plan (SMP) for information security implementation in ITO. During this phase, an extensive ISRM approach is required to identify, analyze, response and monitor risks. Proposed conceptual framework adopts the Malaysian Public Sector Information Security Risk Assessment Methodology (MyRAM) (MAMPU, 2005b) for possible risks identification and analysis. Figure 4 shows the steps for identification and analysis of risks adopted from MyRAM.

Responses/treatments refer to countermeasure that reduces information security risks associated with specific threats such as risk reduction, assignment/transference, avoidance or acceptance. These countermeasures can minimize the impact of information security risks to an organization's data/ information assets. An appropriate risk monitoring approach will ensure the effectiveness of information security countermeasure implementation in the Contract Management and On-Going Monitoring stage within IT outsourcing cycle.

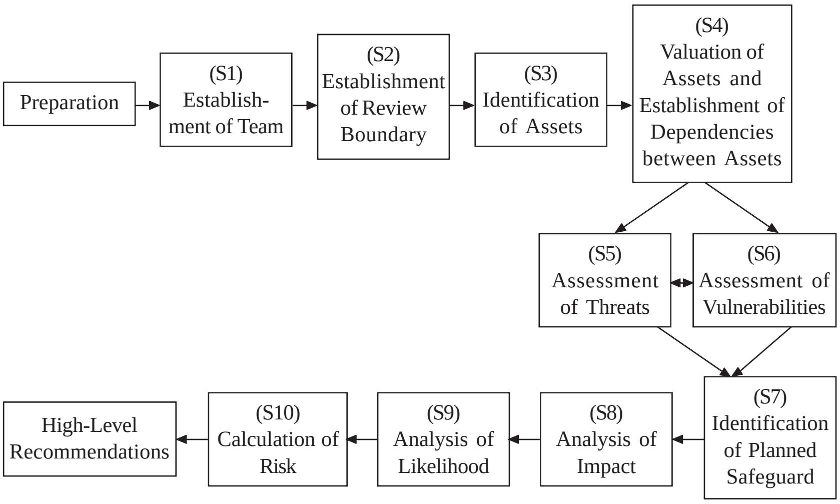
Preparation
(S1) Establishment of Team
(S2) Establishment of Review Boundary
(S3) Identification of Assets
(S4) Valuation of Assets and Establishment of Dependencies between Assets
(S5) Assessment of Threats
(S6) Assessment of Vulnerabilities
(S7) Identification of Planned Safeguard
(S8) Analysis of Impact
(S9) Analysis of Likelihood
(S10) Calculation of Risk
High-Level Recommendations

Figure 4: Information Security Risk Identification and Analysis Process

Conclusion

In direction to minimize the information security risk in IT outsourcing, security measures or control to the risks are needed to address at least one of three principles of information security which are confidentiality, integrity and availability. All countermeasures must be able to protect the confidentiality, preserve the integrity and promote the availability of data for authorized use. Information Security Risk Management approach is the key element in designing an information security management plan. Therefore, dedicated information security risk management for IT outsourcing will ensure a more effective plan for security management.

The proposed framework provides an extensive approach in managing information security risk in an ITO cycle while improving the method of risk management approach in dealing with information security risks. The proposed approach is more reliable since it is also supported by theoretical framework and it complements each other.

By doing so, identification of the risks is controlled in an efficient manner as a key component for effective security management plan.

This framework emphasizes the importance of risk management as the method that links information security governance and IT outsourcing and thereby resolves the often conflicting objectives of information security and value delivery in IT outsourcing.

References

Alberts & Dorofee (2002). *Framework for Managing Information Security Risk*. Addison-Wesley.

Anita & Les Labuschagne (2005). *A Framework Comparing Information Security Risk Analysis Methodology*.

Appin Security Group (2009). Information Security Management. Retrieved on 14/02/09 from http://www.appinlabs.com/ information-security.php

Aubert, B. A., Patry, M. & Rivard, S. (2005). A Framework for Information Technology Outsourcing Risk Management. *The Database for Advances in Information Systems*, 36(4).

Bitha, J. & Von Solms, R. (2004). *A Cycle approach to business continuity planning. Information Management & Computer Security*, 4(4): 328.

Blakley, B., McDermott, E. & Geer, D. (2001). *Information Security is Information Risk Management*.

Chen, T. M. (2006). *Information Security and Risk Management*.

Davison, D. (2003). Top 10 Risks of Offshore Outsourcing. Retrieved from http://techupdate.zdnet.com/techupdate/ stories/main/ op_10_Risks_Offshore_Outsourcing.html

Dhar, S. & Balakrishnan, B. (2006). Risk, Benefits and Challenges in Global IT Outsourcing Perspective and Practices. *Journal of Global Information Management*, 14(3): 39-69.

Engardio, P. & Kripalani, M. (2006). Information Week Research Firm, Research Report 2006.

Garfinkel, S. (2007). All Your Data Belongs to Us: Data Servicing is another problem for data privacy. Retrieved from http:// www.technologyreview.com/blog/garfinkel/ 17585/

Gordon, L. A., Loeb, M. P. & Sohail, T. (2003). A framework for using insurance for cyber-risk management. *Communications of the ACM*, 46(3).

Halliday, S., Badenhorst, K. & Von Solms, R. (1996). A business approach to effective information technology risk analysis and management. *Information Management & Computer Security*, 4(1): 19-31.

Hawkins, S. M., Yen, D. C. & Chou, D. C. (2000). Disaster Recovery Planning: A strategy for data security. Information Management & computer Security, 8(5): 222.

Hinson, G. (2008). *Top Information Security Risk for 2008: Information Security Risk*, CISSP Forum, 2008, pp. 5.

Hinson, G. (2008). *Top Information Security Risk for 2008: Information Security Threats*, CISSP Forum, 2008, pp. 2.

International Organization for Standardization (2008). ISO Standards. Retrieved on 04/08/2008 from http://www.iso.org/iso/iso_catalogue/catalogue_tc/ catalogue_detail.htm?csnumber=42107

International Security Technology Inc (2000). *CORA: Cost-of Risk Analysis*.

Jones, A. (2007). A Framework for the Management of Information Security Risk. *BT Technology Journal*, 25(1).

Ju, Mingseong., Kim, Seoksoo & Kim, Tai-hoon (2007). *A Study on Digital Media Security by Hopfield Neural Network,* Lecture Notes in Computer Science. *'Advances in Neural Networks'*, pp. 140.

Kaplan, R. (2005). *Information Security Risk Management Handbook*, CRC Press.

Karabacak & Sogukpinar (2005). ISRAM: Information Security Risk Analysis Methodology. *Elsevier Computer & Security Journal*, 24(2): 147-159.

Levin, M. & Schneider, M. (1997). Making the Distinction: Risk Management, Risk Exposure. *Risk Management Journal*, 44(8): 36-42.

MAMPU (2002). The Malaysian Public Sector Management of ICT Security Handbook (MyMIS).

MAMPU (2005a). *The Malaysian Public Sector Information Security High-Level Risk Assessment (HiLRA) Guide*, Perpustakaan Negara Malaysia. 'High-Level Risk Assessment Steps'.

MAMPU (2005b). *The Malaysian Public Sector Information Security Risk Assessment Methodology (MyRAM)*, Perpustakaan Negara Malaysia, *'Risk Assessment Methodology'*.

McDougal, P. (2003). Outsourcing's on in a Big Way; Communication Convergence, pp. 17.

Merkow, M. & Breithaupt, J. (2005). *Information Security Principles and Practices.* Prentice Hall.

Miller, L. & Gregory, P. H. (2008). CISSP for Dummies. Wiley Publishing, Information Security and Risk Management, pp. 139.

NISER (2003). Information Security Management System (ISMS) Survey.

Noor Habibah Arshad, Yap, May-Lin., Azlinah Mohamed and Sallehidding Affandi. (2007). Inherent risks in ICT outsourcing project. *Proceeding of the 8th Conference, 8*, 141-146.

Schirripa, F. & Tecotzky, N. (2000). An Optimal Frontier. *The Journal of Portfolio Management*, 26(4): 29-40.

Sota, Teiji (2004). Plagiarism in the age of Electronic Publishing. Population Ecology, 46(3): 219.

Stolen et al. (2003). *UML and the Unified Process*, RMI Press. *'The CORAS Methodology: model-based risk management using UML and UP'*, pp. 332-357.

Stoneburner, G., Goguen, A. & Frenga, A. (2006). *Recommendations of the National Institute of Standards and Technology,* NIST, *'Risk Management Guide for Information Technology Systems'*.

Suh & Han (2003). *Information System (IS) analysis based on a business model*.

Syaripah Ruzaini Syed Aris, Noor Habibah Arshad & Azlinah Mohamed (2008). Conceptual Framework for Risk Management in IT Outsourcing. *WSEAS Transactions on Information Science and Applications,* 5(4): 816-831.

Tipton, H. F. & Krause, M. (2008). *NSW Information Security Guidelines*, Government Chief Information Office.

Tohmatsu, D. T. (2000). Risk Survey 2000

Vassiliadis, B., Fotopoulos, V., Ilias, A. & Skedras, A. N. (2005). Protecting Intellectual property Rights and the JPEG2000 Coding Standards. *Advances in Informatics, 3746*, pp. 705-715.

Vorster, A. & Labuschagne, L. (2005). A framework for comparing different information security risk analysis methodologies. *Paper presented in* the *Proceedings of the ACM Annual Research Conference of the South African Institute of Computer Scientists and Information Technologists (SAICSIT 2005)*, pp. 95-103.

Wawrzyniak, D. (2006). *Lecture Note in Computer Science*, Springer Berlin. *Information Security Risk Assessment Model for Risk Management.*