13

Understanding Components of IT Risks and Enterprise Risk Management

Abdul Rahman Ahlan and Yusri Arshad
Department of Information Systems,
Kulliyyah of Information and Communication Technology
International Islamic University Malaysia,
Malaysia

1. Introduction

There is no doubt that information technology (IT) or information system (IS) improves the efficiency and efficacy of our daily lives. IT derives much of its usefulness from the ability to link systems together to improve functionality and communications (Ahlan, 2005). Inherent in these links are interdependence, interoperability and interconnectedness (O'Brien, 1996). Traditionally, IT is perceived to take the role of back-end support system to an organisation and thus, has little strategic value. Nowadays, this perception has changed primarily due to the potentials that pervasive IT can provide to all aspects of daily profitable organisations', communities' or individuals' efficiencies and efficacies and ultimately to achieve strategies and objectives. IT innovations facilitate all these ever increasing sophistication of IT users (Ahlan, 2005).

Nonetheless, the rapid adoption of IT poses organisations particularly to increasing and excruciating complex and sophisticated risks whether inherent or external. IT security, or risk, has been a highlight of every organisation since the inception of computer systems. Different organisations bear different sensitivity to particularly data and information risks and exposures to technical, organisational, project and human's risks (Wei *et al*., 2010; Ahlan *et al.,* 2011). Manufacturing environment, for example, is less sensitive to information risk compared to healthcare and education sectors which in turn less sensitive compared to banking and finance sector. Universities data and information are highly sensitive and the risks are high. The more IT-laden organisations the more IT risks they are subjected to. Moreover, IT hardware, software and systems are becoming more sophisticated and expensive. Likewise, hackers or computer intruders and fraudsters are also becoming more sophisticated and constantly one step ahead of technology (Gerace and Cavusoglu, 2009). Hence, this puts pressure on manufacturers and service providers as well as IT managers to continuously increase the quality and security of their products and services.

Hence, this study aims to synthesise the risk factors associated with IT/IS and categorise or classify them into a few main major themes to guide the IT management in their risk management exercises. This chapter is organised into five main sections. First, the chapter begins with introduction to IT and risk in general. Second is the description of

methodological approach, review of literature on and description of IT risk, factors and enterprise risk management. Third is the result and discussion of IT risk classification identified from the reviewed articles. Finally, the chapter ends with a brief description of future work.

2. Literature review

Extant literature shows that IT/IS has improved significantly compared to twenty years ago. As technology and systems become more complex and sophisticated, the risks associated to them are also increasingly growing and sometimes more difficult to detect. Different organisations bear different sensitivity to data and information risks and exposures to technical, organisational, project and human's risks (Wei *et al*., 2010; Ahlan *et al.,* 2011).

To ensure a systematic review of the state of the art literature, we follow the approach suggested by Webster and Watson (2002). In a first step, we searched the online database Proquest or ABI/INFORM, ScienceDirect, Emerald and the ACM Digital Library using the search terms "IT risk", "IT security" and "IT risk management" in the abstract, title and keywords. We had to limit to "information technology" in the search in order to reduce the number of articles found which are not relevant to "IT". The articles selected were published from 2001 to 2011. However, a review of the articles revealed that not many articles focused specifically on IT risk factors and enterprise risk management. In a second step we filtered the identified articles according to those in Association for Information System (AIS) journal rankings and book publications. In addition, we also included a few important relevant articles published earlier than 2001 and those from other field such as business, management, operation research journals and conference proceedings. Hence, we reviewed in total 46 relevant articles directly related to IT risks which are tabulated in Table 2 in Appendix. The summary of IT risks categories are tabulated in Table 1. Next sections briefly present review on IT/IS risks and management from literature. The sections are organized according to topics found in the literature.

2.1 Information system and technology roles and risk exposures

Information system plays an important role in any modern organisations to support its strategic, tactical and operational levels activities. These systems are at the core of the information management of the organisations and allow them to operate efficiently and maintain their competitive advantage. Three vital roles of IS, but not limited to, include (i) Support of business operations; (ii) Support of managerial decision making; and (iii) Support of strategic competitive advantage. According to (O'Brien 1996, p.7), ''if IS do not properly support the strategic objectives, business operations or management needs of an enterprise, they can seriously damage its prospects for survival and success''.

Recently, advances in IT have exposed the IT departments, infrastructures, functions and services to more threats from internal and external risks. These threats can be detrimental to not only technical aspects but also the data and information in the organisations which can be costly and even cause terminal loss or bankruptcy. Hence, recognising IT as a technology with the fastest rate of development and application in all branches of business, requires adequate protection to provide high security and quality products and services. The aim of

the safety analysis applied on an IS is to identify and evaluate threats, vulnerabilities and safety characteristics. Moreover, IT assets are exposed to risk of damages or losses. In addition, IT/IS security also involves protecting information stored electronically. That protection implies data integrity, availability and confidentiality.

For example, numerous government reports in United States published over the last few years indicate that federal automated operations and electronic data are inadequately protected against information risks. These reports show that poor security program management is one of the major underlying problems (GAO, 1999). A principal challenge many agencies face is identifying and ranking the information security risks to their operations which is the first step in developing and managing an effective security program. Taking this step helps ensure that organisations identify the most significant risks and determines what actions are appropriate to mitigate them (Ahlan *et al.*, 2011).

In addition to information risks, most security incidents today are caused by flaws in software, called vulnerabilities. It is estimated that there are as many as 20 flaws per thousand lines of software code. Computer Emergency Response Team/Coordination Center (CERT/CC), United States statistics reveal that the number of vulnerabilities reported has increased dramatically over the years, from only 171 in 1995 to 8,064 in 2006. Along with vulnerabilities, the sophistication of attack tools has also advanced over time. Using the interconnected nature of the Internet and automated attack tools, attackers exploit software vulnerabilities at an alarming rate to cause serious damage to organisations (Gerace and Cavusoglu, 2009).

Nowadays, there are many types of computer crimes reported in the United States such as money theft (44%), damage of software (16%), theft of information (16%), alteration of data (12%), theft of services (10%) and trespass (2%) (Boran, 2003). This is also happening in other countries. Hence, in order to minimise losses, it is necessary to introduce risk management and risk assessment in the areas of IT and operational risks. The objective of IT/IS risk management is to protect IT/IS assets such as data, hardware, software, personnel and facilities from all external (e.g. natural disasters) and internal (e.g. technical failures, sabotage and unauthorised access) threats so that the costs of losses resulting from the realisation of such threats are minimised (Gottfried, 1989).

There are myriad dimensions to the complexity associated with protecting our interconnected IS from the technical, managerial, organisational, institutional, cultural, and international political perspectives. This reality makes it difficult to understand the complex interconnectedness of these IS (Longstaff *et al.*, 2000). Modelling and subsequently assessing and managing the risks that face these infrastructures are thus a formidable task. Each dimension is important and must be addressed. However, only when we analyse all the important aspects and perspectives in a complete vision can we make appreciative progress towards the infrastructures' protection and sustained operation. According to (Longstaff *et al.* 2000), we can broadly categorise the complexity of interconnected infrastructures as structural-based, which includes hardware, structures and facilities, and human-based, which includes institutions, organizations, culture and language. There is a dangerous disconnect among the professionals from the multiple disciplines that conceive, plan, design, construct, operate, maintain, and manage these complex infrastructures.

2.2 IT risk and management

IT risk management (RM) and risk assessment (RA) are the most important parts of Information Security Management (ISM). The important step in risk management cycle is risk identification which is to be done comprehensively and iteratively. This chapter, therefore, aims to synthesise the risk factors associated with IT and categorise or classify them into a few main major themes to guide the IT management in their risk management exercises.

2.2.1 IT risk definitions

Various fields such as IT, Engineering, Banking, Insurance, Economics, Management, Medicine and Operations Research have studied risk and risk management in their own domains. Nonetheless, each field addresses risk in a fashion relevant to its object of analysis and, hence, adopts a particular lens of viewpoint. Therefore, the authors will present here some of the risk definitions used in the different fields and relate them to IT risk used in this study.

- Generally, risk occurs in a situation when decisions are made knowing the probability of a risk event which shows that the decision maker has more information available than if he did not (Frame, 2003).
- Furthermore, risk, a measure of the probability and severity of adverse effects, is a quantitative entity and in order to manage it we must be able to quantify it. However, quantifying the efficacy of risk assessment and management for software and information assurance in a well-defined metric (one that others can apply, duplicate and compare) has proven difficult. We have made great progress in quantifying all kinds of risk but not in quantifying the true value of risk to information integrity or to infrastructure protection (Longstaff *et al.*, 2000). In other words, risk is also taken to be a negative outcome or event that has a known or estimated probability of occurrence based on experience or some theory (see, for example, Charette, 1991;Willcocks and Margetts, 1994).
- For example, medicine often focuses solely on the probability of a disease's occurrence (e.g., heart attack), since the negative consequence is death in many cases. It would be useless to focus on the consequence itself since it is irreversible. Odds of occurrence are the key element. Data is used to determine which factors can influence those probabilities (heredity, smoking habits, cholesterol level and others). In its definition of sentinel events (occurrence involving death or serious injury), the Joint Commission on the Accreditation of Healthcare Organisations uses "risk" as "the chance of serious adverse outcome" (Kobs, 1998 as cited by Longstaff *et al.*, 2000). Life insurance adopts this approach 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.
- Levin and Schneider (1997 as cited by Aubert *et al.*, 2005) define risks as "… events that, if they occur, represent a material threat to an entity's fortune" (p.38). Using this definition, risks are the multiple undesirable events that may occur. Applied in a management context, the "entity" would be the organisation. Given this perspective, risks can be managed using insurance, therefore compensating the entity if the event

occurs. They can also be managed using contingency planning, thus providing a path to follow if an undesirable event occurs. This definition of risk is analogous to the concept of risk as a possible reduction of utility discussed by (Arrow 1983).

- On the other hand, finance field adopts a different perspective of risk. They view risk as 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 (Aubert *et al.*, 2005). Risk is defined here as the volatility of a portfolio's value (Levine, 2000). Risk management means arbitrating between risk and returns. For a given rate of return, managers will prefer lower volatility but would be likely to tolerate higher volatility if the expected return was thought to be superior. Portfolio managers therefore aim to build a portfolio that is on the efficient frontier, meaning it has the highest expected return for a given level of risk, and the lowest level of risk for a given expected return (Schirripa and Tecotzky, 2000).
- Other fields, such as casualty 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). Car insurance is a good example. In the eventuality of an accident, there is a loss function that represents the extent of the damages to the car, which can range from very little damage to the total loss of the car. There is also a probability function that represents the odds that an incident will occur. The expected loss (risk) is the product of these two functions (Bowers *et al.*, 1986).
- Another important distinction in risk analysis is the notion of endogenous versus exogenous risk. Exogenous (or external) risks are risks over which we have no control and which are not affected by our actions. Earthquakes or hurricanes are good examples of exogenous risks. Although we have some control over the extent of damage by selecting construction standards, we have no control over the occurrence of such natural events. Endogenous (internal) risks, on the other hand, are risks that are dependent on our actions. A car accident is an example of risk where a strong portion is endogenous. While a driver has no control over other drivers (the exogenous portion), the probability of an accident is strongly influenced by the driver's behaviour and ability (endogenous). The driver also controls part of the loss function, by deciding to drive an expensive car or a cheap car. This could explain why there is always a deductible amount with car insurance, to ensure that the driver will behave in a way that will minimize the endogenous portion of the risk. By being made responsible for a portion of the damages, the driver is enticed to act with caution (Aubert *et al.*, 2005).

In IT/IS studies, risk has been heavily researched in the areas of software development (see, for example, Boehm 1991; Charette, 1991; Griffiths and Newman, 1996; Lyytinen *et al.*, 1998; Ropponen, 1999) and project management (as examples only see Keil, 1995; Morris, 1996; Willcocks and Griffiths, 1996).

Bahli and Rivard (2003) propose a scenario-based conceptualisation of the IT outsourcing (ITO) risk, wherein risk is defined as a quadruplet comprising a scenario, the likelihood of that scenario, its consequences and the risk mitigation mechanisms that can attenuate or help avoid the occurrence of a scenario. This definition draws on and extends a risk assessment framework that is widely used in engineering. The proposed conceptualisation of risk is then applied to the specific context of ITO using previous research on ITO as well as transaction cost and agency theory as a point of departure. Agency theory and

transaction cost theory suggest four main risk scenarios that can be associated with outsourcing: (1) lock-in, (2) contractual amendments, (3) unexpected transition and management costs and (4) disputes and litigation. Resource based view theory identify risks on competences and capabilities of stakeholders while social exchange theory looks from service receiver-provider relationship exchange during ITO project arrangements (Arshad, 2011).

IT risks are perceived to culminate from the potentials that any undesirable events which can bring losses, threats to privacy and security of data and information and life of organisations and individuals. Raftery (1994) suggests that risk can be quantifiable, and proposes that risk is the actual outcome of an activity deviating from its estimate or forecast value. Risk may, therefore, be expressed as an exposure to economic loss and gain. As can be seen, the differences between risk and uncertainty events lie in the (in)ability to know their probability and to quantify their attributes.

In other words, IS has long been at some risk from malicious actions or inadvertent user errors and from natural and man-made disasters. In recent years, systems have become more susceptible to these threats because computers have become more interconnected and, thus, more interdependent and accessible to a larger number of individuals. In addition, the number of individuals with computer skills is increasing, and intrusion, or "hacking," techniques are becoming more widely known via the Internet and other media (GAO, 1999).

Let us consider a technology selection scenario. In a study, (Cochran 2006) suggests that when consumers are confronted with technology decisions, these technology attributes (interdependence, interoperability, and interconnectedness) must be considered. As the numbers and types of information technologies continue to multiply every year, selecting the "right" product is getting more difficult. Thus, for academics, for instance, trying to understand the factors motivating particular technology selection decisions, this becomes a significant yet complex issue.

Cochran (2006) asserts that there are three high level assessment areas in making technology decisions: "standalone" product assessment, technical compatibility assessment, and technology survivability assessment. This is shown in Figure 1. This is because practitioners making technology selection decisions cannot afford to make selection decisions based on the product alone. They must be concerned with whether the product will be compatible with or disrupt existing technologies already in place in the organisation. For example, the "best" technology according to its features and functionality may be extremely expensive to implement if it has incompatibilities. Decision makers must also worry about the survivability of the technology in the marketplace in order to avoid being "stranded" without support. An implemented technology could lose much of its value if the vendor folds or is acquired by another company. Furthermore, there are switching costs inherent in these technology decisions that must be considered. The model, however, does not focus on IT risk criteria or risk theories.

Furthermore, (Cochran 2006) differentiates between technical- and social compatibility. Technical compatibility refers to the capability of multiple products to work together. For example, "will this software package operate on the computer systems we have?" Social compatibility refers to "the degree which an innovation is perceived as consistent with the existing values, past experiences, and needs of potential adopters." For example, "will this

software alter the way that the organisation orders supplies?" or "will this software be compatible with the existing knowledge of the end user?"

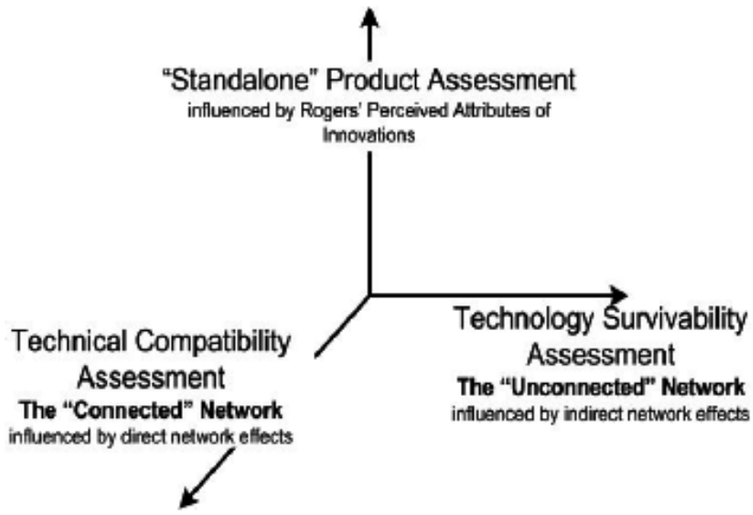


Fig. 1. Technology Evaluation Axis

Based on open-ended interviews of six Chief Information Officers (CIOs), project managers and similar positions, the informants have already indicated the complexities that these decisions entail, as well as the areas that are most difficult to assess. Notably, they have stressed the difficulty in assessing the full impact of the compatibility issue, as well as the difficulty in predicting the future of technologies. Furthermore, they discussed the consequential effects that previous infrastructure decisions can have on current and future decisions.

Thus, without thorough understanding of the factors that must be considered, outcomes of the selection decisions are more uncertain. Once the factors are understood, strategies for better assessment and mitigating risk can be developed. The following section describes the risk management application in IT field decision making process.

2.2.2 IT Risk management decision making

Decision-making takes place in an environment which has three components – certainty, uncertainty and risk (Flanagan and Norman, 1993). While certainty can be thought of as a situation in which all the factors causing a possible event can be exactly specified and known by a decision-maker, uncertainty entails the exact opposite, making an uncertain situation impossible to describe in terms of its probability of occurrence.

Risk management tools take into account whether risk is endogenous or exogenous. In finance, for example, risk is considered exogenous. The methods used to manage risk are concerned with diversification, insurance and allocation of assets. There is no direct action that managers can take to reduce the probability of a given event. In engineering or medicine, a portion of the risk is always endogenous. Risk management takes this into account. Patients are informed of the portion they control and are proposed healthier diets and lifestyles; employees are provided with security guidelines and actions are taken to

reduce directly the probability of undesirable consequences. In IT field, generally, risk management involves analysis or risk identification, planning, implementation, control and monitoring of implemented measurements. Risk Assessment, as part of Risk Management, consists of several processes: (1) Risk identification; (2) Relevant risk analysis; and (3) Risk evaluation. In addition, (Rosman 2008) asserts that the four important aspects of risk management processes include: (1) understanding risk and risk management; (2) risk identification; (3) risk analysis and assessment; and (4) risk monitoring.

Risk management recognises risk, accesses risk and takes measures to reduce risk, as well as measures for risk maintenance on an acceptable level. The main aim of risk assessment, however, is to make a decision whether a system is acceptable and which measures would provide its acceptability. For every organisation using IT in its business processes, it is important to conduct the risk assessment exercise. Numerous threats and vulnerabilities are presented and their identification, analysis, and evaluation enable evaluation of risk impact, and proposing of suitable measures and controls for its mitigation on the acceptable level (Nikolić and Ružić-Dimitrijević, 2009).

In the process of risk identification, its sources are distinguished by a certain event or incident. In that process, the knowledge about the organisation, both internal and external, has an important role. Besides that, past experiences from this or a similar organisation about risk issues are also very useful. There are many techniques for identifying risks available such as checklists, experienced judgments, flowcharts, brainstorming, Hazard and Operability studies, scenario analysis and others (Nikolić and Ružić-Dimitrijević, 2009). In order to assess the level of risks, likelihood and the impact of incidental occurrences could be estimated. This estimation can be based on experience, standards, experiments, expert advice and others. Since every event has various and probably multiple consequences, the level of risk is calculated as a combination of likelihood and impact. Risk analysis or assessment can be either or a mix of quantitative, semi-quantitative or qualitative approaches (Macdonald, 2004).

There are numerous methods applied in risk assessment. In different countries, there are different methods. Even in the same area, there are various methods and applying each depends on a particular occasion. However, the methodology is similar that is system characterisation and description, threat and vulnerability identification, risk assessment, recommended measures and others. The differences in methods are due to the level of development of methodology items. All methods should present common descriptions of threats, vulnerabilities, assets groups and finally, a classification of risks. In that way, they can be compared and in order to achieve the best results, it is useful to apply the combination and optimization of methods. ISO standards for IT security (13335, 17799, and 27001) are general guidelines for implementing the IT security management process but there are no solutions provided on how to conduct it specifically (Nikolić and Ružić-Dimitrijević, 2009). In addition, Sarbanes Oxley (SOX) also requires organisations to assess their IT compliance for reporting purposes. COSO and COBIT are commonly used IT control assessment guidelines in organisations nowadays. Solms (2005) suggest that COBIT (2000) and ISO 17799 (ISO/IEC 17799, 2000) frameworks are complementary and, therefore, are actually very good choices as reference frameworks for Information Security governance. Used together, they provide a synergy which can be very beneficial to organisations.

Thus, implementing a proper risk management approach or technique to manage risks are necessary in today's organisations. The process of risk management is usually divided into risk identification, risk analysis, risk response planning and risk monitoring and control (Hillson, 2002). These steps are sometimes iterative and not always taken in sequence. Generally, it is necessary to express these steps in terms of activities and methods undertaken in the organisations. Once these activities are identified, it is then possible to assess the risk management practices implemented.

The effective management of risk lies in understanding the probability of a risk occurring, and if it does occur, how severe the adverse effect of the risk is likely to be. Between these two domains, risk may therefore be mitigated, accepted, avoided or transferred. In the context of construction, risks may affect cost, quality, safety, environment and time, among others.

External, or global risk, is the risk that falls outside an organisation's control because they arise outside the realm of the organisation's operations (Frame, 2003). Although external risks arise from sources that are different from internal risks, the same risk management principles can be applied to manage them. The management decision pertaining to risks would be dependent on the severity and probability of each particular case of risk. In this context, some risks may be extremely severe if these occur but the probability of their occurrence could be very remote. Consequently, risks may be mitigated, accepted, avoided or transferred as the case may be. In some instances, all aspects of a risk management framework may apply; while in other instances, only selected risk management principles within a framework would suffice. For this reason, it is not possible to tabulate responses to risk management because the spectrum of risks encountered in real life is too diverse and wide ranging to make any tabulation meaningful and succinct. Risk management decisions should therefore be determined on the facts and circumstances of each particular case.

The Project Risk Analysis and Management Guide (PRAM) compiled by the members of the Special Interest Group on Risk Management (APM, 2007) states that implementing a risk management system helps the formulation of more realistic plans in terms of both cost and time estimates. An increased understanding of the risks that might occur and their possible impact which can lead to the minimization of such risks and/or the allocation of these risks to the party best able to handle them is also possible. In addition, an independent view of the risks which can help to justify the decisions and enable the more efficient and effective management of risks are facilitated. Finally, a contribution to the building up of statistical data of historical risks that will assist in such future operations and the facilitation of greater but more rational risk taking and thus increasing the benefits that can be gained from doing so. Sadgrove (1996) adds that risk management helps a company avoid additional costs and disruptions to their operations and identify the risks that are worth pursuing and those that should be shunned. External risk management is especially important also because the firm's operations are now exposed to a dynamic environment influenced by macro-economic, political and social factors.

In any organisations nowadays, IT risk management is enforced at different stage of criticality. In medium to large organisations, enterprise risk management is normally practised in order to mitigate the organisational exposures related to IT risks. This is further explained in the following section.

2.3 Enterprise risk management

The earlier sections elaborated on the importance and steps of IT risk assessment and management in organisations. IT risks are avoidable and unavoidable and therefore, must be managed to minimise the risks. In any organisations, this is known as enterprise risk management (ERM). According to COSO (2004), it is:

- A process, on-going and flowing through an entity;
- Effected by people at every level of an organisation;
- Applied in strategy setting;
- Applied across the enterprise, at every level and unit, and includes taking an entity-level portfolio view of risk;
- Designed to identify potential events that, if they occur, will affect the entity and to manage risk within its risk appetite;
- Able to provide reasonable assurance to an entity's management and board of directors; and
- Geared towards achievement of objectives in one or more separate but overlapping categories

The underlying premise of ERM is that every entity exists to provide value for its stakeholders. All entities face uncertainty and the challenge for management is to determine how much uncertainty to accept as it strives to grow stakeholder value. Uncertainty presents both risk and opportunity with the potential to erode or enhance value. ERM enables management to effectively deal with uncertainty and associated risk and opportunity and thereby enhancing the capacity to build value (COSO, 2004).

Furthermore, according to COSO (2004, p.1), ERM encompasses:

- Aligning risk appetite and strategy – Management considers the entity's risk appetite in evaluating strategic alternatives, setting related objectives, and developing mechanisms to manage related risks.
- Enhancing risk response decisions – Enterprise risk management provides the rigor to identify and select among alternative risk responses – risk avoidance, reduction, sharing, and acceptance.
- Reducing operational surprises and losses – Entities gain enhanced capability to identify potential events and establish responses, reducing surprises and associated costs or losses.
- Identifying and managing multiple and cross-enterprise risks – Every enterprise faces a myriad of risks affecting different parts of the organization, and enterprise risk management facilitates effective response to the interrelated impacts, and integrated responses to multiple risks.
- Seizing opportunities – By considering a full range of potential events, management is positioned to identify and proactively realize opportunities.
- Improving deployment of capital – Obtaining robust risk information allows management to effectively assess overall capital needs and enhance capital allocation.

ERM deals with risks and opportunities affecting value creation or preservation. It is defined as a process effected by an entity's board of directors, management and other personnel and applied in strategy setting and across the enterprise, designed to identify

potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives. Value is then maximised when management sets strategy and objectives to strike an optimal balance between growth and return goals and related risks and efficiently and effectively deploys resources in pursuit of the entity's objectives.

These capabilities inherent in ERM help management achieve the entity's performance and profitability targets and prevent loss of resources. ERM helps ensure effective reporting and compliance with laws and regulations and helps avoid damage to the entity's reputation and associated consequences. In summary, ERM helps an entity get to where it wants to go and avoid pitfalls and surprises along the way (COSO, 2004).

For example, risk management is performed at three levels within Department of Education and Training (DET) (NSW DEC, 2011). These include:

1. Strategic – this relates to risks associated with DET carrying out its business objectives as articulated in the DET Corporate Plan. These risks are identified, documented and managed in the organisation's business plans down to the business unit level (Regions and Directorates). Existing reporting systems are used to report achievement of objectives and management of identified risks.
2. Operational – this relates to the management of risks associated with the DET business units (Regions and Directorates) meeting their specific objectives. These risks are identified, documented and managed in the unit's operational plans. Existing reporting systems are used to report achievement of objectives and management of identified risks.
3. Specialist Areas – to support both Strategic and Operational risk management, DET has established specific policies, procedures and guidelines to ensure effective management of risks relating to:

- occupational health and safety
- child Protection
- serious incidents
- safety and security
- corruption prevention
- business continuity
- environmental management

Section 3 presents the result from the IT risk categorisation and elaborates on each risk categories and examples of situations which the risks might occur.

3. Results and discussion

From the literature analysis, we attempt to provide comprehensive IT risk factors into major IT risk categories. The findings suggest that IT risks generally originate from (I) technical or operational (hardware, software and systems); (II) data and information security; and (III) organisation, project, legal and human or people sides. This is further elaborated under each category in the following sections. Due to a large number of relevant literatures available, we only provide a non-exhaustive list of selected literature for the categorical risk example which is shown in Table 1 below.

Author(s)	Journal/Book (Year)	Risk types/issues	Categories
L.P. Willcocks, M.C. Lacity and T. Kern	Journal of Strategic Information Systems (1999)	Type and scope of outsourcing, vendor selection criteria and process, the role of the contract, retained capabilities and management processes, and partnering and relationship dimensions	II, III
Bunmi Cynthia Adeleye, Fenio Annansingh and Miguel Baptista Nunes	International Journal of Information Management (2004)	Strategic and operational risks which may have considerable financial and reputation costs.	I, III
Ward and Griffiths	Book (2001)	Not achieving the planned benefits, not meeting agreed deadlines, using more resources than initially foreseen, change in functional an procedural requirements, budget overrun and deficient change over of systems and problems associated with the operation and maintenance of these systems.	I, II, III
Kweku-Muata Osei-Bryson and Ojelanki K. Ngwenyama	European Journal of Operational Research (2006)	IS outsourcing contracts	I, II, III
Tafti, M	Industrial Management & Data Systems (2005)	Contracts, privacy and security, technical returns, loss of IT expertise, hidden costs and outsourcing decision process.	I, II, III
Kroenke	Book (2009)	Incorrect data modification, data disclosure and technological security	I, II, III
Rao	EDPACS (2004)	Technological security and legal/political issues	I, III
Ramanujan & Jane	Journal of American Academy of Business (2006)	Incorrect data modification, data disclosure and legal/political issues	II, III
Bouchaib Bahli and Suzanne Rivard	Omega (2005)	Transaction,client and supplier sources	II, III
Kakoli Bandyopadhyay, Peter P. Mykytyn and Kathleen Mykytyn	Management Decision (1999)	Application level, organizational level and interorganizational level.	I, III
Melinda Cline, Carl S. Guynes and Andrew Nyanoga	Journal of business and economic research (2010)	Environmental conditions and changes, organisational conditions and changes, managerial cognition, managerial actions, changes in the content of strategy and organisational outcomes.	III

Author(s)	Journal/Book (Year)	Risk types/issues	Categories
Fariborz Farahmand, Shamkant B. Navathe, Gunter P. Sharp and Philip H. Enslow	Information Technology & Management (2005)	Network system threats [(1)Threat agent: Environmental Factors, Authorized users and Unauthorized users and (2) Penetration technique: Physical, Personnel, Hardware, Software and Procedural].	I, III
Benoit A. Aubert, Michel Patry and Suzanne Rivard	The DATA BASE for Advances in Information Systems (2005)	Principal, agent and transaction categories.	II, III
Barki, H., Rivard, S., and Talbot, J.	Journal of Management Information Systems (1993)	Technological newness (need for new hardware, software), application size (project scope, number of users, team diversity), expertise (lack of development expertise, task of application-specific expertise, lack of user experience), application complexity (technical complexity, links to existing legacy systems), organizational environment (task complexity, extent of changes, resource insufficiency, and magnitude of potential loss).	I, II, III
Boehm, B.W.	IEEE Software (1991)	Software risk factors, including personnel shortfalls, unrealistic schedules and budgets, developing the wrong functions, developing the wrong user interface, "gold-plating," a continuing stream of changes in requirements, shortfalls in externally furnished components, shortfalls in externally performed tasks, performance shortfalls, and strained technical capabilities.	I, III
McFarlan, F.W.	Harvard Business Review (1981)	Dimensions of project risk based upon project size, experience with the technology, and project structure.	I, III
Keil, Mark., Cule, Paul E., Lyytinen, Kalle and Schmidt, Roy C.	Communications of the ACM (1998)	Four quadrants of risks including risks associated with customer mandate, scope and requirements, execution, and environment.	II, III
Thomas A. Longstaff., Clyde Chittister, Rich Pethia and Yacov Y. Haimes	Journal of Computer (2000)	Risk in systems integration: software development, temporal, leadership, environment, acquisition, quality and technology	I, II, III

Table 1. Risk types/factors (includes IT/IS outsourcing, investment, project management)[1]

[1] Note: For Summary of Risk Factors in Information Systems Projects (1983-1997), see Mary Sumner (2000), 'Risk Factors in Enterprise Wide Information Management Systems Projects'. Association of Computing Machinery (ACM).

3.1 Technical and operational risks

- Large IT risks originate from technical or operational risks in hardware, software and systems. In hardware, this can be in terms of faulty or defect products that can affect other hardware and systems within the same or networked environment. Even though manufacturing warranties do cover products defects after purchases, electrical short circuit in the hardware, for instance, could pose threats to other hardware, software and systems as well as data and information.
- Furthermore, the complexity of our technological organisation and society has forced us to deal with coupled and interconnected systems of systems whose likelihood of failure is ever increasing. The dominance of IT in our business and commerce has also created an almost critical-path dependency across our interconnected IS and critical infrastructures. For example, banking and finance institutions depend on the information infrastructure to operate their systems, reliable telecommunications depend on electricity and the electric utilities depend on a reliable source of energy. This networked systems and environments apply to most organisations nowadays even to small businesses with peer to peer or client-server and shared computers and peripherals.
- Therefore, computer security has become an important issue in this networked environment. The proliferation of personal computers, local area networks and distributed processing has drastically changed the way we manage and control information resources. Internal controls that were effective in the centralised, batch-oriented mainframe environment of yesteryears are inadequate in the distributed computing environment of today. Attacks on computer systems and networks are on the rise and the sophistication of these attacks continues to escalate to alarming levels. As more organizations share information electronically and autonomous computer networks work their way into our everyday lives, a common understanding of what is needed and expected in securing information technology resources is required.
- This is because the world of computers has changed dramatically over the decades. Twenty years ago, most computers were centralised and managed by data centers. Computers were kept in locked rooms and staffs of people made sure they were carefully managed and physically secured. However, in the computing world of today, autonomous network communications are setting the standards on how we interact with one another in a global environment. An effective security plan can successfully provide adequate safeguards to protect an organization's vital resources and assets.
- An ineffective security plan increases the economic costs associated with software vulnerabilities. It decreases the efficiency of an organisation and does not protect the resources and assets of the organisation. Inadequate protection of system resources compromises information obtained through email, research data and configuration data, services obtained via IS and applications and equipment such as computers and networking components. In addition, components vital to an organisation such as confidentiality, integrity, authenticity and availability are also compromised.
- Hence, an effective computer security plan protects an organisation's valuable resources, such as information, hardware and software. Furthermore, it also strengthens the aforementioned vital components of an organisation. Through the selection and application of appropriate safeguards, a security plan helps the organization's mission by protecting its physical and financial resources, reputation, legal position, employees

and other tangible and intangible assets. An effective security procedure reduces the economic costs associated with software vulnerabilities.

- For instance, the common threats to IS and computer networks can be classified into the Accidental, Intentional, Passive and Active categories. Accidental threats are losses due to malfunctions or errors. Some examples of accidental threats are power failures, hardware vulnerabilities in network switches, routers and other hardware components, software failures and natural threats such as fires and flooding.
- Intentional threats cause damage or corruption to computer assets. Sabotage is a type of intentional threat that uses small virus programs often propagated by unsuspecting users. Denial of Service (DoS) is another form of intentional threat that causes loss of availability of service. Some examples of DoS include e-mail spamming and network packet attacks aimed at host vulnerabilities.
- Passive threats do not change the state of the system. They may include loss of confidentiality but not the loss of integrity or availability. An example of a passive threat is traffic analysis, a form of eavesdropping in which an analysis of traffic patterns is used to infer information that is not explicit. Another instance of a passive threat is replay which is the repetition of valid messages in order to gain unauthorised access and masquerade as another entity.
- Unlike passive threats, active threats change the state of the system. These include changes to the data and software. Some examples of active threats are Trojan horses and trapdoor software, both of which alter parts of the system to allow unauthorised access. Security threats that are common today differ from those in earlier times. With worldwide Internet connections, anyone can gain access into an organisation's computer system from anywhere in the world and steal passwords although the building may be physically secured.
- Thus, even though physical security accomplished its objective in this scenario, the network is still not secure. Viruses and worms can be passed from machine to machine. Global autonomous networks provide an opportunity for "electronic thieves" to open windows and doors in the computer system's architecture. This "virtual thief" can detect and then exploit vulnerabilities in hundreds of machines in a matter of hours.

3.2 Data and information security risks

- In this information and knowledge era, organisational and individual data and information are available in digital forms. In many instances they are available on networked environement. Thus, they are susceptible to theft, misuse, abuse, modification, improper disclosure, fraud and others. It is, therefore, important that this risk is minimised in any organisation. One important method to curb this risk is through digital certificates and signatures whereby only certified authorised names are allowed to access any particular privileged authorised data and information. Moreover, most organisations nowadays also impose access level security controls on their networks and enterprise resource planning or other systems such as accounting, operations, human resource, marketing and management. Data administrator levels are also controlled between higher, middle and lower level staff. Nevertheless, sophisticated hackers, spyware and other sniffing tools are always on the lookout for data and information intrusions. Thus, IT managers must be constantly alert on any

unusual logging activities in their organisations' systems and servers. Any irregularities must be reported and taken action immediately to avoid foreseeable losses due to data and information theft and intrusions either from inside or outside the organisations.

- Hence, organisations must follow some acceptable international standards and compliance regulations on IT risks and security controls such as ISO, COBIT, COSO and SOX. The purpose of any IT standard is, for example, to provide steps that employees must take to avoid inappropriate release of private and confidential organisational information. The focus of the standard is on the sensitive information that exists in a digital form, whether stored in a database, used in an application, transmitted over a network, or used in a report. Organisations and individuals information must be protected from any inappropriate sharing, releasing or use. When the information exists in a digital or electronic format, additional steps must be taken to ensure the protection of the information from loss, corruption, or inappropriate disclosure.
- Understanding the risks involved in handling information in digital form includes an appreciation of the greatly increased vulnerability made possible by technological conveniences that offer portability, easy copying, and wide—potentially global—distribution. The lack of reliable and current data often precludes precise determinations of which information security risks are the most significant and comparisons of which controls are the most cost-effective. Because of these limitations, it is important that organizations identify and employ methods that efficiently achieve the benefits of risk assessment while avoiding costly attempts to develop seemingly precise results that are of questionable reliability.
- Thus, all organisations and individuals information must be handled with appropriate security and access controls, and with attention to safeguarding confidentiality. No information should be exposed inappropriately. Many data elements and other types of information are protected by each country's current statute or regulation or in Malaysia case such as Malaysia legal acts, Malaysia Communication and Multimedia Commission (MCMC), university acts and others. Information that is not protected by law or regulation should, nonetheless, be protected against inappropriate exposure.

3.3 Organisation, project and human or people risks

- These types of risks originate from or within the organisations, projects and people. In an organisational environment, the policies, procedures, regulations, cultures and others, if not carefully designed, can pose risks to IT environment. Building security, access controls, electrical fittings, for example, can become sources of threats to IT hardware and software. Organisational type, vertical or hierachical, sizes, structures and building occupational health and safety implementation can result in different level of risks. In many organisations that create a proper IT division or department, the risks are minimised by the hands of professionally-trained staff. It is important for all staff to adhere to all IT security and controls policies and guidelines imposed by the management. Therefore, many small organisations are at risk of having their computer systems, hardware and software misused, abused, fraud, improperly installed and others.
- On project risk, the sources of risks can originate from any sources in the project cycles or processes. Project panel and stakeholders must carry out due diligence exercise on

feasibility of projects to reduce risks. IT project management consists of several important stages as stated in Project Management Body of Knowledge (PMBOK® Guide), which is the standard put forward by the Project Management Institute (PMI). They include Initiation, Planning, Execution/Managing and Closing. The guide lists nine elements of project management encompassing Project Integration Management, Scope Management, Time Management, Cost Management, Quality Management, Human Resources Management, Communications Planning, Risk Management and Procurement Management. This stages and processes also apply in any ITO projects.

- While ITO is associated with significant benefits, it can also be a risky endeavour. Researchers and practitioners also recognise that, in some circumstances, ITO entails risk, and that it sometimes leads to undesirable consequences that are the opposite of the expected benefits. In ITO projects, either onshore or offshore, more risks are posed depending on the nature of ITO projects themselves. Among the major risks are in selecting the right providers, win-win terms and conditions in contractual documents, access to organisational buildings and information privileges and project management service deliveries. In many ITO literatures, many projects failed due to poor project management, contract clauses and cultural differences in the case of offshoring. Relationship between service receiver and provider is also crucial for ITO success. ITO failure is not much attributed to technology but more on human competence, capabilities and relationship. Moreover, risk in systems integration, including software development, temporal, leadership, environment, acquisition, quality and technology, could become major sources of risks in IT and ITO projects (Arshad, 2011).
- Furthermore, since ITO projects involve relevant stakeholders within and outside the organisations, these human or people risks add more to inherent IT risks in the projects. Lack of commitments, understanding, competence and capabilities and communications, for example, can increase ITO project risks. In addition, staff within an organisation can also involve in stealing private and confidential information, hardware and software, improper usage, maltreatments, carelessness and other damages to IT hardare, software, systems and information. (See Sumner (2000) for further reading on IS project risk factors).
- Finally, IT risks originating from human or people could be attributed to human errors and misbehaviours. Competence and capabilities distinguish each staff in their work professionalism. As in ITO projects, human or service provider-receiver relationship is crucial for ITO project success. These can be found in many ITO literature. Human's attitude such as greedy, carelessness, selfish and others can increase IT risks in any organisations.

The previous section divides and elaborates IT/IS risks into three types: 1) Technical and operational risks; 2) Data and information security risks; and 3) Organisation, project and human or people risks. IT risk nature depends largely on types of assets or projects. Each IT hardware, software, system or project has its own inherent and incidental risk associated to it. Uncertainty presents both risk and opportunity, with the potential to erode or enhance value. Therefore, any organisation must undertake a risk assessment and management initiative to minimise risks that could result in big potential losses. Enterprise risk management enables management to effectively deal with uncertainty and associated risk and opportunity, enhancing the capacity to build value.

4. Future work and closure

Risk is a common terminology adopted in every field including IT/IS. While many definitions offered from different perspectives, IT risk in this study adopt the definition of IT risk being the uncertainty that a foreseeable loss or damage can result for such uncertain probabilistic events.

IT risk nature depends largely on types of assets or projects. Each IT hardware, software, system or project has its own inherent and incidental risk associated to it. This chapter classifies IT risk into three types, namely: 1) technical and operational risk; 2) data and information security risk; and 3) organisation, project and human risk.

Uncertainty presents both risk and opportunity, with the potential to erode or enhance value. Therefore, any organisation must undertake a risk assessment and management initiative to minimise risks that could result in big potential losses. Enterprise risk management enables management to effectively deal with uncertainty and associated risk and opportunity, enhancing the capacity to build value.

In short, aligning organisational strategy with IT strategy could help manage IT risks in the organisation. Organisational strategy must acknowledge the potential IT risks associated to all organisational assets that can increase its liabilities. Continuous IT risk assessment and management exercise, not only identify and minimise IT risks at an early stage and manage them, but also facilitate and help achieve the overall organisational short, medium or long-term goals and strategies.

Finally, organisations may opt to undertake ERM exercise for better control IT risks and security. The sooner, continuous and consistent applications of ERM can significantly minimise calculated risks and increase the profitability of organisations which in turn will be ploughed back into the organisations, staff, communities and stakeholders.

This study provides the theoretical foundation on IT risk components. While IT risk studies have been carried out based on a researcher's theoretical framework, our next initiative is to perform multiple case study using mixed and multi method research in Malaysian organisations context to explore on the IT risks in practices. Another possible study is to perform comparative practices between developing and developed world organisational contexts.

5. Acknowledgment

This study is funded by Malaysia Ministry of Higher Education (MOHE) under Fundamental research grant scheme FRGS 10-029-0148. We would like to thank to International Islamic University Malaysia, Research Management Centre (RMC) for their kind assistance. Finally, our sincere gratitude goes to the organisations and respondents who contribute to the study directly or indirectly.

6. Appendix

Table 2 below lists the relevant articles reviewed in this study. While most of them represent articles found in the AIS journals, the authors, however, also include other relevant articles found in books and conference proceedings in order to enrich the sources for the literature review. The articles were published from 1991 to 2011.

Journal / Book / Proceedings	Year
Book - Course Technology, Cengage Learning	2011
Wireless Network	2011
ACM Computing Surveys	2011
Information Privacy & Security	2010
Business & Economics Research	2010
Proceeding of ACM New Security Paradigms Workshop (NSPW)	2010
IEEE Security and Privacy	2009
Consortium for Computing Sciences in Colleges	2009
Proceeding of IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology - Workshops	2009
Systems and Software	2008
Communications of the ACM	2008
Information security technical report	2008
The VLDB	2008
Consortium for Computing Sciences in Colleges	2008
Assocation of Computing Machinery	2006
Consortium for Computing Sciences in Colleges	2006
Proceeding of ACM International Conference on Privacy, Security and Trust	2006
ACM Special Interest Group on Management Information Systems	2006
Proceeding of InfoSecCD Conference	2006
European Journal of Operational Research	2006
Strategic Information Systems	2005
Computers & Security	2005
Omega	2005
Information Technology and Management	2005
Information Security Curriculum Development (InfoSecCD) Conference	2005
Proceeding of 7th International Conference on Electronic Commerce, ICEC	2005
The DATA BASE for Advances in Information Systems	2005
Computers & Security	2004
International Journal of Information Management	2004
Sixth International Conference on Electronic Commerce, ICEC	2004
International Journal of Information Management	2004
Information Management & Computer Security	2003
Pers Ubiquit Computing	2003
Consortium for Computing Sciences in Colleges	2003
Information Technology	2000
IEEE Computer	2000
ACM SIGCPR Computer Personnel	2000
Supply Chain Management: An International Journal	2000
Information Management & Computer Security	1999
Management Decision	1999
Strategic Information Systems	1999
Supply Chain Management: An International Journal	1999
MIS Quarterly	1998
ACM Computing Surveys	1993
Management Information Systems	1991
IEEE Software	1991

Table 2. Related articles under review

7. References

Ahlan, A. R. (2005). Information technology implementations: Managing IT innovation in the Malaysian commercial banking industry. Unpublished doctoral dissertation, University of Cardiff, United Kingdom.

Ahlan, A. R., Arshad, Y. & Lubis, M. (2011). Implication of Human Attitude Factors Toward Information Security Awareness in Malaysia Public University. Proceedings in International Conference on Innovation and Management (IAM2011), Kuala Lumpur, Malaysia.

APM (2007). Project Risk Analysis and Management Guide, second edition. Association for project management (APM).

Arshad, Y. (2011). IT Outsourcing decisions and implementations in Malaysia public healthcare sector agencies: Grounding an ITO relationship model using qualitative approach. Unpublished doctoral dissertation. International Islamic University Malaysia.

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

Bahli, B. & Rivard, S. (2003). The information technology outsourcing risk: a transaction cost and agency theory-based perspective. Journal of Information Technology, 18, pp.211–221.

Bahli, B. & Rivard, S. (2005). Validating measures of information technology outsourcing risk factors. Omega, 33, pp.175 – 187

Barki, H., Rivard, S., & Talbot, J. (1993). Toward an assessment of software development risk. Journal of Management Information Systems, 10(2), pp.203-225.

Benoit A. Aubert, Michel Patry & Suzanne Rivard (2005) A Framework for Information Technology Outsourcing Risk Management. The DATA BASE for Advances in Information Systems, 36(4), pp.9-28.

Boehm, B.W. (1991). Software Risk Management: Principles and Practices. IEEE Software, 12, pp.32–41.

Boran, S., (2003). IT security cookbook. Boran Consulting.

Bouchaib Bahli & Suzanne Rivard (2005) Validating measures of information technology outsourcing risk factors. Omega, 33, pp.175 – 187.

Bunmi Cynthia Adeleye, Fenio Annansingh & Miguel Baptista Nunes (2004) Risk management practices in IS outsourcing:an investigation into commercial banks in Nigeria. International Journal of Information Management, 24, pp.167–180.

Cochran, J. (2006). A Comprehensive Model for Understanding Technology Selection Decisions of Interconnected Information Technologies, Proceedings of SIGMIS-CPR'06, April 13–15, 2006, Claremont, California, USA.

COSO (2004). Enterprise Risk Management — Integrated Framework: Executive Summary. By Committee of Sponsoring Organizations of the Treadway Commission.

Fariborz Farahmand, Shamkant B. Navathe, Gunter P. Sharp & Philip H. Enslow (2005) A Management Perspective on Risk of Security Threats to Information Systems. Information Technology and Management, 6, pp.203–225.

Flanagan, R. & Norman, G. (1993). Risk management and construction, Blackwell Scientific Publications, London.

Frame, J.D. (2003). Managing risk in organizations: A guide for managers, Jossey-Bass, NY, US.

GAO/AIMD-00-33 (1999). Information Security Risk Assessment, Practices of Leading Organizations. A Supplement to GAO's May 1998 Executive Guide on Information Security Management. United States General Accounting Office, 1999 [ai00033.pdf]

Gerace, T. & Cavusoglu, H. (2009). The Critical Elements of the Patch Management Process. Communications of the ACM, 52(8).

Gottfried, I.S. (1989). When disaster strikes. Journal of Information Systems Management, pp.86-9.

Hillson, D. (2002). Extending the risk process to manage opportunities. International Journal of Project Management, 20, pp.235–240

June Wei, Jason O'Connell, & Meiga Loho-Noya (2010) Information Technology Offshore Outsourcing Security Risks and Safeguards. Journal of Information Privacy & Security, 6(3), pp.29-46.

Kakoli Bandyopadhyay, Peter P. Mykytyn & Kathleen Mykytyn (1999) A framework for integrated risk management in information technology. Management Decision, 37(5), pp.437-444.

Keil, Mark., Cule, Paul E., Lyytinen, Kalle & Schmidt, Roy C. (1998). A framework for identifying software project risks. Communications of the ACM, 41(11), pp.76–83.

Kroenke, D. (2009). Using MIS. Upper saddle river: Pearson prentice hall.

Kweku-Muata Osei-Bryson & Ojelanki K. Ngwenyama (2006) Managing risks in information systems outsourcing: An approach to analyzing outsourcing risks and structuring incentive contracts. European Journal of Operational Research, 174, pp.245–264.

Longstaff, T.A., Chittister, C, Pethia, R. & Haimes, Y.Y. (2000). Are We Forgetting the Risks of Information Technology? Journal of Computer.

Macdonald, D. (2004). Practical machinery safety. Pondicherry, India: Integra Software Services.

McFarlan, F.W. (1981). Portfolio approach to information systems. Harvard Business Review, 59(5), pp.142–50.

Melinda Cline, Carl S. Guynes & Andrew Nyanoga (2010) The impact of organisational change on information systems security. Journal of business and economic research, 8(1), pp.59-64.

Nikolić, B. & Ružić-Dimitrijević, L. (2009). Risk Assessment of Information Technology Systems. Issues in Informing Science and Information Technology. 6, pp.595-615.

NSW DEC (2011). Enterprise Risk Management in the Department of Education and Communities.
https://www.det.nsw.edu.au/policies/general_man/erm/PD20040036.shtml
accessed on 31st October 2011.

O'Brien, J. A. (1996). Management information systems: Managing information technology in the networked enterprise. Boston: McGraw-Hill.

Raftery, J. (1994). Risk analysis in project management, E & FN Spon, London.

Ramanujan, S. & Jane, S. (2006). A legal perspective on outsourcing and offshoring. Journal of American academy of business, 8(2).

Rao, M. (2004). Key issues for global IT sourcing: country and individual factors. EDPACS, 32(4), pp.1-12.

Rosman, R. (2008). Risk Management and Performances of Islamic Banks: A Proposed Conceptual Framework. 2008 EABR & TLC Conferences Proceedings.

Sadgrove, K. (1996). The Complete Guide to Business Risk Management. Aldershot: Gower.

Solms, B. V. (2005). Information Security governance: COBIT or ISO 17799 or both? Computers & Security, 24, pp.99-104.

Straub, D.W., & Welke, R.J. (1998). Coping with Systems Risks: Security Planning Models for Management Decision Making, MIS Quarterly, 22(4), pp.441-469.

Tafti, M. (2005). Risks factors associated with offshore IT outsourcing. Industrial management and data systems, 105(5), pp.549-560.

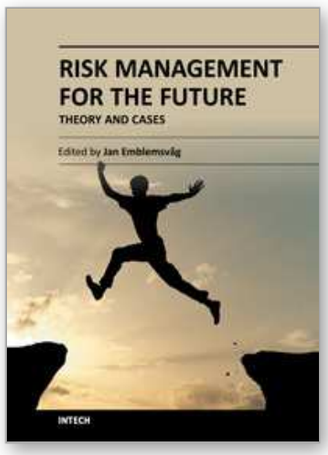
Thomas Gerace & Huseyin Cavusoglu (2009). The Critical Elements of the Patch Management Process. Communications of the ACM, 52(8).

Ward, J., & Griffiths, P. (2001). Strategic planning for information systems. Chichester:Wiley.

Webster, J., & Watson, R. T. (2002). Analysing the past to prepare for the future: Writing a literature review. MIS Quarterly, 26(2), pp.13-23.

Whitman, M. E., & Mattord, H. J. (2004). Management of Information Security. Boston: Thompson Course Technology.

Willcocks, L.P., Lacity, M.C. & Kern, T. (1999). Risk mitigation in IT outsourcing strategy revisited: longitudinal case research at LISA, Journal of Strategic Information Systems, 8, pp.285–314.



Risk Management for the Future - Theory and Cases
Edited by Dr Jan Emblemsvåg

ISBN 978-953-51-0571-8
Hard cover, 496 pages
Publisher InTech
Published online 25, April, 2012
Published in print edition April, 2012

A large part of academic literature, business literature as well as practices in real life are resting on the assumption that uncertainty and risk does not exist. We all know that this is not true, yet, a whole variety of methods, tools and practices are not attuned to the fact that the future is uncertain and that risks are all around us. However, despite risk management entering the agenda some decades ago, it has introduced risks on its own as illustrated by the financial crisis. Here is a book that goes beyond risk management as it is today and tries to discuss what needs to be improved further. The book also offers some cases.

How to reference
In order to correctly reference this scholarly work, feel free to copy and paste the following:

Abdul Rahman Ahlan and Yusri Arshad (2012). Understanding Components of IT Risks and Enterprise Risk Management, Risk Management for the Future - Theory and Cases, Dr Jan Emblemsvåg (Ed.), ISBN: 978-953-51-0571-8, InTech, Available from: http://www.intechopen.com/books/risk-management-for-the-future-theory-and-cases/understanding-components-of-it-risks-and-enterprise-risk-management-a-literature-review

INTECH
open science | open minds

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821

IntechOpen