MÄLARDALEN UNIVERSITY SWEDEN

School of Sustainable Development of Society and Technology

MASTER DEGREE PROJECT

Critical Factors for Effective Information Systems Risks Management

D level	15 ECTS
Term:	Spring 2011
Author:	Ahmed Abd Elkhalek
Supervisor:	Ph.D. Peter Ekman
Examiner:	Professor Ole Liljefors

Mälardalen University

School of Sustainable Development of Society and Technology.

IT Management master degree.

Master Thesis in IT Management.

Course Code: EIK034

Abstract

The rate of information systems and/or information technology failures even with the existence of risk management models which are to help reduce IT failures necessitated this thesis. To reduce the IT failures, companies need to understand that different critical factors such as involving both risk management staff and non risk management staff underlie effective risk management. This essay presents a coherent theoretical framework of the critical factors for successful risk management, for instance, educating non risk management on risk identification and monitoring and choosing risk management models according to certain qualities, from various scientific articles within IT/IS research. The theoretical framework was put to test by collecting empirical data through structured interviews of various managers with titles such as Chief Information Officer, Chief Technology Officer (CTO), and IT manager and so on responsible for risk management issues in ten (10) purposefully sampled IT projects in Egypt.

The findings of this study indicate that critical factors have specific impact on risk management models and effectiveness of risk management in general. Specifically, we found that critical factors such as the essential features of information system: technology, information, people, and system-hardware and software; the qualities of risk models: clarity, practicality of use, completeness and adaptability; effective communication between risk management staff and other staff; and proper coordination of the resources in organizations are important to effective risk management as indicated by the responses of the interviewees. In the same vein, our findings indicate that the extent to which companies' apply risk management frameworks depends on the companies' identification of their major risks and the difficulty in managing them. Furthermore, the study also found that language and political risks to be critical factors for risk management in Egypt. In sum, this paper found that effective risk management depend on underlying critical factors which governs risk management issues from risk management models' selection to models' application in practical risk management environments.

Acknowledgements

First and foremost, I would like to express my deepest gratitude to my supervisor Ph.D. Peter Ekman for his inestimable support that enabled me to complete this thesis. I am equally indebted to Professor Ole Liljefors for his evaluation of this thesis and the suggestions offered.

Secondly, I am equally thankful to the interviewees for their invaluable input without which this document wouldn’t have been possible.

Last but not the least; I am also sincerely thankful to my friends and family for their encouragements and other forms of support that helped me to produce this essay.

Table of Contents

List of Figures

1 Introduction

In this contemporary information era, as there is increasing investment in Information Technology (IT) companies (Belle, Eccles, and Nash, 2003; Applegate, Austin, and McFarlan, 2007; Symantec, 2008), Information System (IS) risk management has a critical role to play in protecting IS assets. Thus information system risk management lie at the heart of the success and profitability of IT companies. Prior reports and/or articles suggest risk management processes by which projects including information system risks can be managed (James, 2003; ExecutiveBrief, 2008; Hillson, 2010). The suggested risk management processes can reasonably be considered as benchmarks for managing IS risks in IT companies. However, considering the dynamic nature of IT and its inherent risks and especially as researchers such as Saur and Cuthbertson (2003) and Bronte-Stewart (2009) present data on increasing failures of IT/IS projects, it is intriguing to try to investigate critical factors that contribute to achieving successful risk management in practice.

1.1 Background and Research Area

Risk management is an indispensable part of every organization and a mechanism by which impacts of threats (or risks) are identified, assessed, and minimized and opportunities for gains are seized (ExecutiveBrief, 2008; Jutte, 2010). Consequently, risk management is crucial for the efficient operation of the information systems of an organization. Information system is defined as an interface between people and IT that enhances an effective gathering, processing, storing, and transmission of organizations' information and provide feedback mechanism which helps an organization to achieve its goals (Belle, Eccles, and Nash, 2003; Ralph, George, and George, 2009). Applegate, Austin, and McFarlan (2007) point out that both opportunities and threats are created as a result of the relentless pace of the IT evolution. It implies that information system risk has equally relentlessly evolved since the information system is a product of people's use of IT to provide the information needs of organizations.

Information system risk management is defined here as the process by which potential risks of an information system are identified, assessed, and systematically controlled and/or mitigated to enable an organization achieve its goals (James, 2003). From the premise made above about the evolution of the information system risk as IT evolves means that information system risk is dynamic and hence its management must equally be dynamic if organizations want to stay in business. The question as to how information systems risks are managed in a constantly changing world of IT arise logically.

Various explanations and/or models regarding risk management in information technology projects and/or companies have been offered by the contemporary literature on risk management. Apostol-Maurer (2008) discusses that an efficient concept of risk management based on information systems that optimize on the flow of information is an effective risk management model for companies. Radack (2009) offers the National Institute of Standards and Technology (NIST) risk management framework as an effective way to manage information systems risks. The NIST’s framework provides a structured process and information that helps organization to be able to indentify information system risks, assess the risks, and take systematic steps to mitigate the risks (Radack, 2009). On the other hand, Olzak (2008) offers a modified version of the NIST’s framework (making it a generic model) for both private and public organizations. Olzak (2008) claims that the NIST’s framework focuses on how the U.S. government operates hence the need for the modification. Other frameworks offered by other authors include but not limited to the Enterprise Risks Management (ERM) (Shaker, 2010); and the ten golden rules for successful risk management in projects (Jutte, 2010). All the models are well framed for risks managers to adopt and apply in managing risk in their companies. However, literature on problem-solving in IT suggests a different approach. Hedman and Kalling (2002) point out the importance of strategy in IT firms and discuss that strategy is a problem-solving process, as firms deal with specific problems as they occur: that is practical problems. Thus problem-solving in IT should be based on the IT environment. The environment of IT is an ever changing one (that is IT is very dynamic). If information systems operate in the same dynamic environment as IT then information system risk management will equally be dynamic in response to specific information system risk as they occur and will involve the consideration of many important factors rather than just the risk management approaches. Risks is often dynamic and may have different meanings to different people albeit the use of risk as a universal concept for threats and loss. Kloman (1990) explains that different users of risk often attach different meanings to it, though it looks like a universal concept. Therefore, it is not enough for firms to simple adopt risk management models; firms understanding of the nature of risk and hence the critical factors for risk management are important to reduce the rate of risk management failures shown by various scientific evidences.

The rate of failures of IS/IT projects due to risk management problems, even with the existence of the risk management models, is unimaginable. For instance, according to Standish Group (2001) quoted in Tiwana and Keil (2004) in U.S. it cost companies as much as $75 billion annually due to large numbers of IT projects' failures from risk that could be assessed and managed. The rate of success of IT projects is estimated at 34%, 15% failures, and as much as 51% projects suffering from cost and time overruns (Standish Group, 2003 in Al-Shehab, Robert & Graham, 2005). Similar revelations include as much as 142 billion Euros loss in information systems failures across European Union due primary to poor and/or lack of stakeholder communication within the projects community as well as the wider management hierarchy (John and Trevor, 2007). Saur and Cuthbertson (2003) in Bronte-Stewart (2009) list projects' failures from various sources including but not limited to an Oxford survey report which shows just 16% IT project were successful, and as much as 74% were "challenged" with 10% abandonments. Apparently, the data presented here questions not only the effectiveness of risk management models, but also suggests that effective risk management is more a matter of many critical factors such as effective communication which guide both the understanding of risk and its environment and the strategy to manage to the risk. Kloman's (1990) discussions of various connotations of the risk and Hedman and Kalling's (2002) presentation of strategy as a problem-solving process of firms give an idea that firms consider many important factors in risk management.

The present research tries to investigate risk management in practice and especially the factors that contribute to effective risk management. This is the basic problem which this essay is concerned and hence tries to investigate. To be specific, it is hypothesized in this essay that if information system risks is as dynamic (relentless pace) as it has been described analogous to Applegate, Austin, and McFarlan description of IT then effective IS risks management in practice will require fundamental factors that will play crucial roles in making risk management effective. Challenges that contemporary information system risk management models encounter in practice will be considered in the light of the critical factors that risk managers need to consider.

This study makes contribution to literature in the following ways. Firstly, it investigates how risk managers are able to cope with the complexities and dynamic nature of risk in practice. IT project failures have been the talk of many studies therefore the way risk management is done in practice is worth investigating. Secondly, this essay collects data from Egypt by which may reveal some vital information about risk and its management in non-Western country.

1.2 Problem Statement and Research Purpose

In theory there are many well formulated risk management frameworks for IT managers to use in managing information systems risk. However, given the statistics of IT projects failures found in the literature, this is essay proposes to investigate how IT risks are managed by companies in practice.

It follows from above that, this essay would attempt to answer the following questions:

1. What are the critical factors for information systems risk management?
2. Do threats impact on the extent to which risk management frameworks are used?
3. How do companies attempt to increase the effectiveness of their risk management approaches?

Answering the questions posed above would deepen our understanding about the risk management processes in practice. This essay would hopefully provide rich source of information especially with regards to fundamental factors that underlie successful risk management.

1.3 Limitations of the Essay

The scope of this research is based mainly on investigation and analysis of critical factors for effective information system risks management in IT projects in Egypt. Thus, the results obtained may not be applicable to other types of risks managed by other IT projects in other countries. There may also be some difficulty in gathering all the necessary empirical data from the anticipated number of companies hence limiting the amount of empirical data to be presented.

1.4 Essay Outline

The rest of the essay shall be discussed in four chapters. Chapter 2 presents the methodology applied to answer the research questions. The methodology chosen for the empirical data collection, the sample size of the data, and the place for the data collection shall be presented. This essay uses structured interviews to gather the empirically data. This approach is chosen because our main interest is to evaluate crucial factors necessary for effective risk management in practice. The theoretical framework comprising the features of information systems, qualities of good risk management models, IS risk management models, and a generic risks management frameworks shall be presented in chapter 3. The discussion presented in chapter 3 is meant to elicit the nature of IS risk and the proposed risk management models in the IS literature, to enable us investigate the extent of the application of the risks management models in practice. The generic risk management framework which will mirror the risk management models identified and shall be presented using the framework of Schlaak et el. (2008, pp.3-4). Empirical results from the interviews and analysis shall be presented in chapter 4. The conclusion and discussion shall be presented in chapter 6. The implications of our findings as well as areas that need further research shall be presented as well in this chapter.

2 Research Methodology

This research work is based on deductive approach because we are concern with the possible link between risk management in theory and in practice: hence it requires methodology of inquiry that can be used to gather data from the experiences of risk management practitioners. In order to learn the subtle difference between theory and practice of IS risk management in IT companies, it is important to present relevant theoretical discussions connected to risk management in the IS literature and then conduct an investigation to bring forth practitioners actual practices which enable us to confirm or refute the theories presented. Practitioners' actual practices in this context is analogous to what Argyris & Donald (1978) labelled as people having mental maps that enables them in specific situations and most importantly the mental maps guide practitioners' actions rather than the theories they espouse explicitly to. Thus, this essay conducts two parts of research: conceptualization part and confirmatory part. The conceptualization and confirmatory parts fall under the deductive approach because as Gill and Johnson (2002 in Pathirage, Amarantunga, and Haigh, 2008) assert that "*a deductive research method entails the development of a conceptual and theoretical structure prior to its testing through empirical observation.*" Deductive approach is helpful where new and more coherent framework is needed to explain a problem which is not adequately explained by contemporary frameworks. Pathirage, Amarantunga, and Haigh (2008) discuss that the emphasis in deductive approach is the deduction of new ideas or facts from the new conceptual and theoretical framework in the hope that it provides explanation to a problem than preceding theories. This thesis is concern with the issue of increasing risk management failures even with the existence of explanations of how risk could be managed effectively and so the deductive approach is robust for the issue under consideration.

The conceptual and theoretical part discusses the nature of IS risks and the requirements risk management models must meet to be useful in managing IS risk in practice. Risk management models discussed in the IS literature will be identified and presented. It should be made clear that the processes in individual models will not be discussed but rather a set of generic risks management processes which corresponds to the processes in individual models. The discussion of the generic processes rather than the processes in individual models is based on the framework presented by Schlaak et el. (2008, p.3-4). Since this research' goal is not test a particular risk management model but to rather find out risk management models IS risk managers are assumed to espouse to, presenting the models in the present framework matches with the goal. Consequently, the information gathered and presented in this part will enable us to find out which of the risk management models are used in practice, the extent of the usage of risk management models, and the critical factors that underlie effective risk management in the confirmatory part.

Structured interview shall be conducted in the confirmatory part to find out how risk managers are guided in practice that is either by their experience or theory and/or both. Since our attempt is to answer questions such as "What are the critical factors..." posed in this essay, the confirmatory approach is a perfect approach to enable us confirm or refute the critical factor we deduced and discussed in the theoretical framework.

A purposeful sampling would be used to gather the data since our interest is in IT projects. Ten (10) IT projects representing the population of IT projects in Egypt would be sampled to gather an information rich empirical data set through a structured-interview technique. Maxwell (1997) discusses that purposeful sampling is useful in situations where particular events or persons should be deliberately selected for information which cannot be gotten from other sources apart from the sample selected. There are many international and national IT projects in Egypt. All the companies selected for the interview have good reputation, in and outside Egypt, based both on their histories and their performances, hence gathering data from risk managers in Egyptian IT projects offers a quality data set. Furthermore, the blend of national and international companies might reveal something interesting about differences in risk management. The researcher would first contact risk managers, Chief Information Officer (CIO), Chief Technology Officer (CTO) or some application/software manager in IT companies identified to discuss the research, the intended structured interview, and discuss the possible date on which the interviewed can be conducted. The structured interview questions will be delivered to the respective interviewees a day before the date for the interview: to enable the interviewees to acquaint themselves with the questions and for the interviewer to confirm the possibility of the interview the next day. Then the next stage follows, that is the interview is conducted according to the dates agreed with each interviewee. The interviews are face-to-face and expected to take between thirty to forty minutes. The interview will take place in Cairo, Egypt at smart village: a place where all technological projects have their headquarters. The purpose of the research, the importance of responding, assurance of confidentiality: companies will be labelled with letters in the data presentation and analysis, and the non transferability of the information will be expressed at the beginning of every interview.

2.1 Reliability and Validity

Reliability is concern with the extent to which research findings are free from errors that is consistent (Golafshani, 2003). The nature of the interview questions used to conduct the interviews makes it possible to obtain similar responses over time in the same setting that is, with the representatives of the companies interviewed in Egypt. As Miller (n.d.) points out that a response to certain questions such as “What do you like to eat more, pizza or hamburgers?” would probably be stable over time and thus enhances the reliability of the findings. Ensuring the reliability of our interview is very important as that is fundamental to the validity of a research. According to Nunnally (1978 cited in Hinkin, 1995, p.979) reliability is a necessary pre-condition for validity.

Validity of research of a research is the degree to which the research measures what it intends to measure, and construct validity is one form of validity which is applied to test (Ridley, 2005) and/or give assurance about research validity. This essay employs Hazel’s (2006) findings as the instrument to validate the research being undertaken by this paper. Hazel finds, in support of Keil et el. (1998) and Cule et el. (2000), that practical solution is necessary for the inherent difficulty in the formal prescription of risk-by-risk planning. Hazel’s (2006) research indicates the impact of managers’ experience on risk management and problem solving strategies. Hazel concludes that even though managers relied on broad general strategies; however, the strategies derived from risk managers’ experience impacted on their ability to manage the complexities and risks inherent in IT projects: thus experience is fundamental to effective management strategies. Therefore this finding establishes a relationship between theory and practice risk management, which this essay is concerned with. According to Ridley (2005) construct validity can be applied if previous research findings establish a given relationship. More so, using Hazel’s findings as construct validity we can attempt to generalize our findings to IT projects in Egypt. The answers to the questions are given back to each of the respondents to cross check for validation.

3 Theoretical Frameworks

This chapter presents and discusses critical factors such as the essential features of IS and the qualities of a good risks management model for effective risk management. An overview of risk management models and a generic model as a representative of the overviewed risk management models are also presented. The various sections mentioned here are considered as the fundamental structures for risk management.

3.1 Features of Information Systems

The essential features of information system are incorporated into the theoretical framework because their proper identification and their relationships are fundamental to effective risk management: IS features are interconnected and so risk from feature can spread to other features. Vesely and Rasmuson (1984 cited in Alter and Sherer, 2004) discuss that even the most refined risk assessment used to develop accident scenarios in complex [...] systems, suffer from "completeness uncertainty," uncertainty about whether all significant phenomena and relationships have been considered. Thus, risk managers understanding of the essential features of the information systems enables them to identify common threats to each feature and the relationships between the threats of the individual features thereby reducing the degree of uncertainty. As Tversky and Kahneman (1974 cited in Alter and Sherer, 2004) note the high possibility of uncertainty arising from biases that often clouds risk identification.

This essay adopts and modifies the four (4) essential features of IS: Tasks, Information, People, and System (TIPS) discussed by Ferris (2001). This essay felt the need to break the system down into hardware and software: system is broad and encompassing. For instance, the Warning Network of the Royal Army Force which helped the allied force to victory during the Second World War as an early indication of information systems (Beynon-Davies, 2009). Paul stresses the importance of the interaction of people, activities (tasks) and technology, working within a given environment as essential features of information systems. Risk is inherent in the information systems (no system is completely immune from risks) and the context in which it operates. Highlighting software risks (as noted by Sherer and Alter, 2004, pp.29-64) alone logically exclude other IS risks which then leads to biasness in risk identification and consequently to risk management failures. Risks may persist not because they cannot be managed but because they are not identified and assessed for mitigation. Identification of risks in each of the interfaces of information systems leads to an efficient information system risk management. Thus, successful information systems risk management depends on the proper identification of the essential features of a firm's information systems.

3.2 Qualities of Risk Management Model

The qualities of what is considered a good risk management model are important in risk management. To manage the inherent risks in information systems, Alter and Sherer (2004, pp.1-28) suggest that risks management models must satisfy certain criteria. Alter and Sherer emphasis that good risks management model must meet these qualities. The required criteria by the two researchers are presented below:

- **Clarity**: A good risk management model should be conceptually clear
- **Practicality of use**: Risk managers should find the model intuitive and trustworthy and be able to use it in practice.
- **Completeness**: The model should not omit any relevant issue that risk managers care about. It should cover all relevant issues in information systems in this case our TIPS framework. That is, any model which excludes certain IS features put not just those excluded at risk but the whole IS at risk since the whole system is both an interface and interconnected.
- **Adaptability**: The model should be environmentally adaptable. It should be possible for users to be able to include and/or exclude certain components of the model to adapt it to their particular needs and/or situation; but they should be aware of both the advantages and disadvantages of the adaptation. This thesis will use adaptable interchangeable with adjustable or flexible.

The four qualities presented above complement each other: that is risk managers need to choose models that mirrors all the four qualities. Thus, a model that meets all the four qualities increases the effectiveness of risk management.

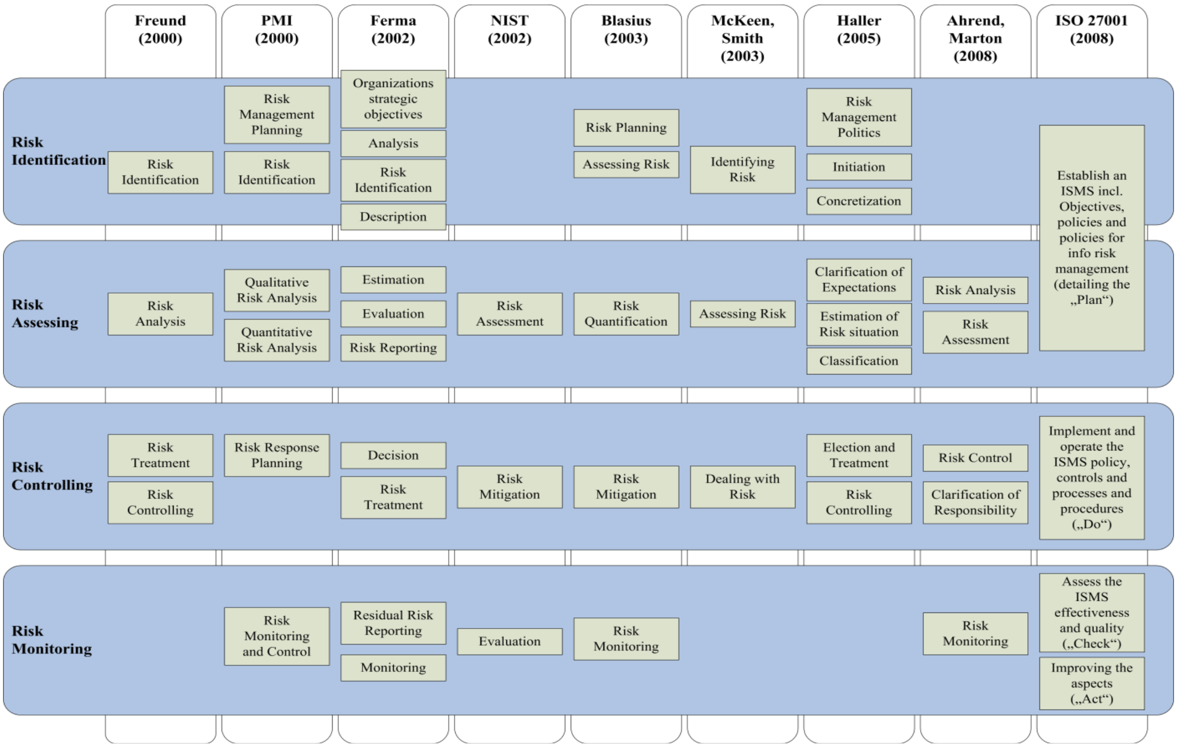
3.3 Information Systems Risk Management

This essay does not attempt to propose a theoretical management model for information systems risk management for IT companies or test the effectiveness of a given model; but rather to find out the extent of usability of existing theoretical management models in practice. Therefore, an overview of theoretical risk management models found in the literature and an ideal way risk can be managed are discussed here. A generic risk management model is used to show the ideal way risk can be managed. It is assumed that the essential features of IS are identified and that the risk management model chosen by a risk manager meet all the four criteria of a good model presented earlier.

Risk management is an integral part of every organization's strategic management (AIRMA, IRM & ALARM, 2002). It is processes by which organizations methodological address the inherent risks in its activities using both tactical and systemic approaches with the goal of achieving sustain benefits from each activity and across all portfolios of activities (AIRMA, IRM & ALARM, 2002; Alberts and Dorofee, 2009). Tactical approach is bottom-up that is identification of all risks that can affect a program's performance and issuing statement separately for each risk; while systematic approach is top-down that is a holistic view of risk identification by top management (Alberts and Dorofee, 2009). While Alberts and Dorofee (2009) see systemic approach to be easier and hence preferred, this essay considers the two approaches not to be substitutive (they are not competitive) but necessarily complementary approaches in risk management: risk is uncertain if it were certain then top managers could just assemble them and manage them at once. However, since they can occur at anytime and any part of an organization's information systems selecting one approach may be a risk factor by itself. Thus it is crucial to coordinate the efforts of all employees labelled in this essay as risk management synergies by combining both the tactical and systematic approaches for effective risk management. Risk management synergies in analogous to Jones (2010, p.404) discussion of information synergies will occur when top management allow employees and/or subunits to adjust their actions to the needs of their fellow employees and/or subunits in an ongoing basis that will enable better risk management from team-based cooperation. Furthermore, employees need to be given some basic knowledge about risks in their respective subunits to enable them inform top management of any suspected risks. Thus even if a team is constituted and given the responsibility of managing an organization's risks, the team has to collaborate with other non risk management employees: thus communication should be both ways. It is noted in the IS/IT literature that most project failures come from badly managed communication and/or lack of risks communication (Bronte-Stewart, 2009; Jutte, 2010). That is, given employees basic information about risk as well as encouraging them to report any risks coupled with the top management's efforts on risk management increases the effectiveness of risk management.

3.2.1 Risk Management Approaches

The overview of various risk management approaches presented by Schlaak et el. (2008, p. 3) in Figure 1 below and the Project Risk Analysis and Management (PRAM) guide (Shaker, 2010), Enterprise Risk Management (ERM) (PricewaterhouseCoopers LLP, 2004) as well as Australia/New Zealand Standards 4360 (AS/NZS 4360) framework discussed by Yusuff (n.d.) are adopted as the list of risk management models for risk management. The risk management approaches were surveyed from the literature on risk management in information technology and information systems and thus assumed to be a good representation of different approaches to risk management in information systems. The idea is to find out the models which are in use by firms: that is in theory these are the models that firms need to use to manage their risk.



	Freund (2000)	PMI (2000)	Ferma (2002)	NIST (2002)	Blasius (2003)	McKeen, Smith (2003)	Haller (2005)	Ahrend, Marton (2008)	ISO 27001 (2008)
Risk Identification	Risk Identification	Risk Management Planning Risk Identification	Organizations strategic objectives Analysis Risk Identification Description		Risk Planning Assessing Risk	Identifying Risk	Risk Management Politics Initiation Concretization		Establish an ISMS incl. Objectives, policies and policies for info risk management (detailing the „Plan“)
Risk Assessing	Risk Analysis	Qualitative Risk Analysis Quantitative Risk Analysis	Estimation Evaluation Risk Reporting	Risk Assessment	Risk Quantification	Assessing Risk	Clarification of Expectations Estimation of Risk situation Classification	Risk Analysis Risk Assessment	
Risk Controlling	Risk Treatment Risk Controlling	Risk Response Planning	Decision Risk Treatment	Risk Mitigation	Risk Mitigation	Dealing with Risk	Election and Treatment Risk Controlling	Risk Control Clarification of Responsibility	Implement and operate the ISMS policy, controls and processes and procedures („Do“)
Risk Monitoring		Risk Monitoring and Control	Residual Risk Reporting Monitoring	Evaluation	Risk Monitoring			Risk Monitoring	Assess the ISMS effectiveness and quality („Check“) Improving the aspects („Act“)

Figure1. Overview of different Risk Management approaches [Source: Schlaak et el. (2008, p. 3)]

3.2.2 Generic Risk Management Processes

The generic risk management framework is presented by discussing: Risk Identification, Risk Assessment, Risk Controlling, and Risk Monitoring as processes that mirror the processes of each of the models presented by Schlaak et el., 2008 in the figure 2. The approach taken to present our framework meets the requirement of the aim that we set in this paper: the fundamental ways of managing each of the stages in a risk management framework in practice. Thus the factors that provide the foundation for effective risk management at each stage of the risk management processes are identified and discussed.

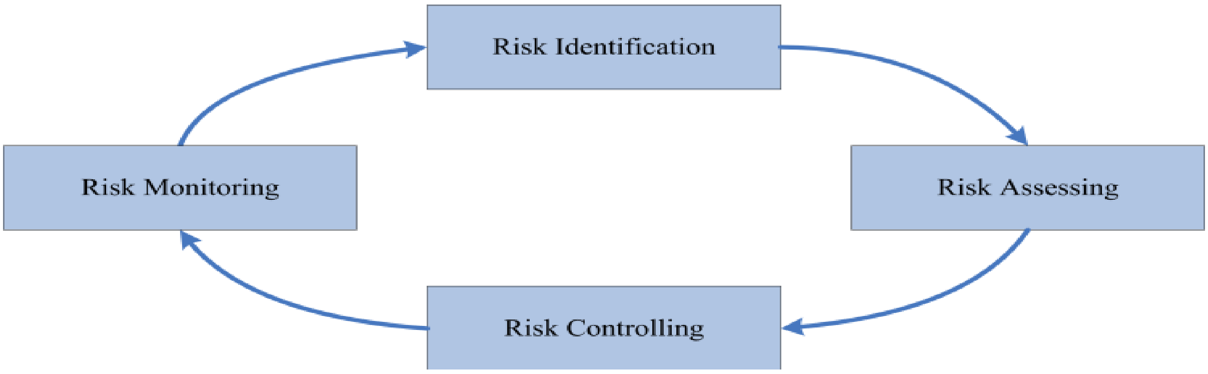


Figure2. General Risk Management Cycle [Source: Schlaak et el. (2008, p. 4)]

Risk planning is recommended as the first step of the risk management process (Ferris, 2001; James, 2003; Wrona, 2008); however, James (2003) puts it that planning should begin during the project selection stage. Our focus is on existing IT companies and their risk management processes hence risk identification is a perfect first step to consider. There is no risk to assess and manage without first identifying them. The difficulty in identifying risks to some extent is one of the main reasons why risk management is not done properly and hence why so many projects have failed (James, 2003). Consequently, risks identification is first (Jutte, 2010) and should be done in a team (collective knowledge and experience of a group such as through brainstorming in another sense team learning and system rather than bureaucratic attributes) (James, 2003; Bolfíková, Hrevova, and Frenova, 2010, pp.135-163). The team learning and system approach of risk identification is in line with the proper flow of communication between both bottom-up and top-down discussed earlier. The identification can also be done in a methodological way to ensure risks' factors related to all the essential features are identified and all their risks defined. The team approach needs to be complemented with methodological approach to risk identification to reduce the difficulty in identifying risks. Furthermore, risk arises from both internal and external sources hence identification of internal risks such as the insider threats to the information systems and external risks such as hackers are critically important. Thus, effective risk identification is fundamental effective risk management.

Risk assessment is the second important step after risk identification. Since the bottom-line of every business is profitability which risk has the potential of turning into loss, then assessing these risks and subsequently managing them is very important. When risks are identified then establishing their probability of occurrence and their consequences should become paramount. The risks matrix suggested by ExecutiveBrief (2010) could be used to assess risk likelihood and consequences as well as their severity. Another method of assessing risk is cause-and-effect (also called Ishikawa) (James, 2003). The Ishikawa approach is very important if risk managers are to get input from all the essential features of information systems: it lends itself to brainstorming and team development (James, 2003). Each of the two has a weakness such as the matrix is quantitative and thus could yield inaccurate results (Yusuff, n.d.) while the fishbone is qualitative that is subjective and thus suffer from the possibility of value judgement. The two techniques are useful in information systems with regards to probabilities (Sherer and Alter, 2004, pp.29-64) of occurrences and effects. Risk matrix and Ishikawa need to complement each other to increase the effectiveness of risk assessments. Though risk managers need to be mindful of cost-benefit issues of risk management; however, the application of the two will increase the quality of the risk assessment and hence the effectiveness of risk management.

After going through the process above, the third step is risks control. At this stage management and/or technical techniques should be used to provide some countermeasures or safeguards to manage the risks assessed. An organization can use countermeasures or safeguards including but not limited to practices, procedures, organizational structures, and policies. Organizational structure is particularly important here because it impacts on the procedures, practise and policies in an organization, and they intend to impact on how members of an organization interact with each other and use resources for the common good of an organization. Organizational structure defines the system of task and authority relationships that control how people coordinate their actions and use resources to help achieve the goals of an organization (Jones, 2010, p.29). It is apparent that countermeasures are preventive actions taken against threat to information systems and since organizational structure is one of such actions, it implies that a structure which facilitates an effective flow of communication is a natural candidate for a good countermeasure. The importance of organizational structure in information systems/IT risk control is stressed by Schneider, Lane, and Bruton (2009, pp.63-65). Technological controls such as technology to monitor and manage system performance (performance management), technologies governing access to IT infrastructure and facilities (physical security) (Symantec, 2007, p. 15) and/or through mitigation that is either being able to lessen the probability of the occurrence of risk or transfer the risk to a third party through insurance (Yusuff, n.d.; Randall and Arthur, 2009, pp.58-62). It is important to have countermeasures to ensure that an information system is well safeguarded from threats that may affect it and hence profitability.

The last step on the model presented here is risk monitoring. It is concern, basically, with making sure that the appropriate risks control strategies developed earlier are in place and are practiced. Risk monitoring involves putting appropriate controls in place and insuring that the procedures are understood and followed (AIRMAC, IRM, & ALARM, 2002). Monitoring is also an evaluation of the control measures because managers check to see if the controls are enough or there is the need to add more controls. Monitoring involves determining if the strategies to respond to the risks are adequate (James, 2003). Consequently, risk cues (low, medium, and high) could be developed and used to monitor risk. For instance, if the control measures put in place are working as expected indicates a low risk cue, the control measures are in place but have little effects than as expected indicates a medium risk cue, and the control measures do not offer the safeguards expected indicates a high risk cue. With this monitoring strategies risk managers can act to change controls and/or add more controls if there is indication of either medium of high risk cues.

The steps presented above if followed and implemented well risk inherent in the information systems would be reduced to an appreciable level. However, it is important to add that risk management is a circular process that starts and ends with a project or company. It is a team work even if one person is selected as a risk manager and effective communication in a company is part of each of the risk management steps.

3.2 Summary: Risks Management Framework

Three contributory factors to effective and efficient IS risk management are identified and discussed by this essay. The factors considered are understanding the interconnectedness of the essential features of information systems, knowing the requirements that a good risks management model must meet (a good risk management must possess the criteria presented by Alter and Sherer, 2004), and then choosing one of the risk management processes identified and/or the general risks management circle discussed. Furthermore, qualities of a good risk management models are acting as a mediating factor between the risk management models and effective risk management. Thus the combined impact of these factors provides a framework of critical factors for effective information systems risk management.

4 Empirical Findings and Analysis

The empirical results collected from the structured interviews and the analysis are presented in this chapter. The results presentation will correspond to the each of the sections of the theoretical framework: each section acts as a code and corresponds to the factors that this investigation is interested in. Furthermore, the results of subsections will be presented under the main section. Brief data on the companies and the role of the respondents are presented below. The companies are labelled with letters A-J due to the assurance given that the confidentiality of both the respondents and the companies will be preserved.

Company A: Information Technology Solutions Provider

Company A is a worldwide IT solution (products and services) provider. The company creates, develops, and manufactures the most advance computer systems, software, networking and so on to the IT industry. The company has a network of professionals worldwide that work to make sure that its customers' technological needs are met. The interviewee is the chief information officer (CIO) of the Egyptian branch.

Company B: Information, Communication, and Technology Service Provider

Company B is a multinational telecommunication company that specialises in delivering communication, network, applications, wireless products and services and other related solutions to wide range of organizations. It partners with its clients to make sure that all their ICT needs are met. The interviewee is the project management office professional (PMOP) of the company in Egypt.

Company C: Telecommunication Service Provider

Company C is a major cellular phone service provider to millions of customers in Egypt. Furthermore, it provides wireless service to the Middle East. The company has good ratings from customers' satisfaction and transparency in information disclosure to its stakeholders. It gained prestigious awards in the Telecoms World Awards for Middle East. The interviewee is the head of business solutions development technology in Egypt.

Company D: Communication Service Provider

Company D is an Egyptian company that provides IP services with a national network and regional divisions. The company has carrier-grade IT network equipment that enables the company to have full transit connections to major IT giants for either direct or transit global internet route coverage services. The company is powered by its success in Egypt to roll out its services into other Arab countries. The interviewee is chief communication officer (CCO).

Company E: IT Business Solutions Provider

Company E is a global integrated business software and hardware systems provider. Its product strategy provides adaptability and alternatives to customers' IT infrastructure. The company has a competitive value proposition: well integration of layers to work together as a single system. Its competitive value proposition is further strengthen by its open architecture and multiple operating-system options to its customers. The interviewee is chief technology officer (CTO).

Company F: Information and Communication Services Provider

Company F is an Egyptian company that provides services in audio and radio production. It is one of the largest audio and radio station in the Middle East. The company has very wide listenership so it has many of its programs sponsored by companies such as Mobinil among others. The interviewee is the senior systems administrator.

Company G: IT Business Services Provider

Company G is a huge global IT and network services provider. The company's services include broadband and mobile internet as well as telecom services to other service providers. The network infrastructure of the company is very fundamental to its growth. It offers superior services to its customers. The interviewee is the IT manager in Egypt.

Company H: Banking and Finance Service Provider

Company H is a dynamic and active global banking and financial services organization. The company handles large sums of transaction on the counter and through automated teller machines (ATMs). Furthermore, it handles Money Gram Transfers, sending daily reports on Foreign Exchange, operating buying and selling of foreign exchanges and so on. The companies branches are networked thus making it possible for all its electronic transactions and services to customers to be met. The interviewee is the head of data centre unit, banking technology division in Egypt.

Company I: Banking and Financial Services Provider

Company I is a well networked Multinational Corporation providing a wide range comprehensive banking and financial services to millions of customers. The corporation is well networked not only within Egypt but other of its branches through the world making it possible for it to provide its comprehensive services. The interviewee is the deputy head of the IT division of the bank in Egypt.

Company J: Banking and Financial Services Provider

Company J is an Egyptian bank and financial services corporation. It provides a range of services such as corporate banking, consumer banking, and global transaction services. It has best bank recognition in Egypt and North Africa. The interviewee is senior IT administrator of the corporation.

4.1 Information Systems Risk Management

The empirical results of the information system management shall be presented thematically to match with the various propositions put forward in the theoretical framework and to facilitate the analysis.

All the respondents said they had risk management models more so seven companies (representing 70%) gave names of their risk management models. In addition, nine companies (representing 90%) said they interact with their workers on risk management issues. These findings indicate the importance of risk management to companies. Even if the response given by company F on the interactivity between management and workers on risk management: *"It is new employees that we educate about our policy and the threat environment...mostly our threats are personal in nature born out of news items or announcements by our station. We started streaming on the internet so we are reviewing our threat environment"* is considered, it still shows the importance of risk management and the need to make workers aware of every companies' risk environment and how their input helps in manage it. Company F's statement illustrates an important point about people's reactions to the media in different countries with reference to Western and non-Western countries. Furthermore, the findings also show the reliance of companies on risk management models; however, the models are not followed strictly by companies in some cases as seven companies (representing 70%) said their models are adapted to their own practices and/or specific risk environments. In the same vein, 60% of the companies (6 companies) said adaptability is the quality that motivates them to select a model. The findings of the reliance of many companies on theoretical risk models falls in line with the many models (for instance the overview of risk management models by Schlaak et el., 2008; Enterprise Risk Management (ERM), PricewaterhouseCoopers LLP, 2004)) found in the literature for risk management; however, when the companies' reliance on the flexibility to select their models is drawn into the picture then it raises a question of the identity of the models used for risk management in practice. On one hand, the risk management models that the IT risk management literature mentions have outlined processes (see for instance Schlaak et el., 2008, p.3); on the other hand, their adaptability (flexibility) makes them useful in practical IT risk management environments. A hypothetical question then is: whether it is improper adjustment of the theoretical risk management to fit the practical risk environment that is responsible for the many IT risk (see for instance many IT failures discussed by Bronte-Stewart, 2009) discussed in the literature? Flexibility of a model is a quality not a practice, thus companies may select models based on this quality but the models may not be adjusted well for risk management in practiced.

On the issues of risks management technicalities, four companies (representing 40%) said risk identification, assessment, controlling, and monitoring are essential in their risk management process, two companies (representing 20%) added planning to the four essential processes; and additional two companies (representing 20%) said the essential processes in their risks management are risk identification, assessment, and controlling. These results relate to companies' reliance on the four processes of the generic risk management model and/or a certain combination of it with other processes. It is gathered that nine companies (representing 90%) use multiple approaches in gathering information on risk management. In the same respect, eight companies (representing 80%) said they use both cause-and-effect and risk matrix (where probabilities of risk and threats levels are calculated and documented) to assess their risk. Furthermore, except for company F which uses comprehensive insurance policy and organizational structure that allows for effective communications and the effective use of resources as its countermeasures, the rest said they had all the three countermeasures: organizational structure allows for effective communications and use of resources that lessens risks; technology that monitors and manages the performance of our systems; and comprehensive insurance on our information systems. More so, except for company F all the rest answered affirmative to having risk cues for monitoring of risks. These findings show the importance of the various processes and the extent of their applicability in risk management. As discussed in the framework, the high number of companies' reliance on the various processes, using multiple approaches to gather risk information and putting in place risk cues relate to the effectiveness risk management. The findings fits with the proposition that team based approach such as brainstorming to risk identification, risk matrix and cause-and-effect approaches to risks assessment, organizational structure that allows for proper coordination for the use of resources, and the institution of risk cues increase the effectiveness of risk management (James, 2003; Bolfíková, Hrevova, and Frenova, 2010; ExecutiveBrief, 2010).

4.2 Qualities of Risk Management Models

All the companies excluding D & F said all the four qualities: clarity, practicality of use, completeness, and adaptability were necessary for them to choose their risks management models. Furthermore, adaptability is the favourite quality for the choice of a risk management. For instance, reasons given by companies for relying on adaptability to choose their models include but not limited to:

"...the threat environment is changing day by day...so we need models that are flexible enough to go with the changes." (Company C). In the same vein, company D said *"Risk changes but we can't keep changing different models to match...it takes experience to use models...to keep changing means each time models are going to be new to you and that can reduce your effectiveness...it is adaptability that solves these problems."* Moreover, company H said *"Risks are uncountable and sometimes not even known as it should be...risk management models are countable and have to manage these risks...it is adaptability that makes the models to match with the risks."* These findings indicate that the four qualities of a risk management model as presented in the framework matter to companies and the choice of adaptability (flexibility) as the favourite quality of a model means models' usefulness depends, to some extent, on its applicability in different contexts.

4.3 Features of Information Systems

Seven of the companies (representing 70%) said all the four features: Technology, Information, People, and System-Hardware and Software of information systems were essential to them while two companies: G & I and company F said three features and one feature were essential to them respectively. Furthermore, all companies with the exception of F said technology had innate risks which are difficult to manage. The reasons for the difficulty of managing technological risk were given as costly, uncertainty, and technological interconnectedness. For instance, some of the responses to the cause of the difficulty were *"costly, unpredictable, it's subjected also to global threats and factors that sometimes we can't see"* (company E) and *"network infrastructure is so hard to manage"* (company C). In the same vein, company B said *"the failures are unpredictable [...] uncertainty."* These findings show that companies care about knowing the essential features of the information systems as that helps them to know the risk environment (innate risk) of each and their manageability. The identification of the essential features increases the effectiveness of the identification of risk in information systems: thus knowing the essential features reduces uncertainties that might arise from biases that often clouds risk identification (Tversky and Kahneman, 1974 cited in Alter and Sherer, 2004). In a related finding, the companies said technical factors pose greater threats to them given reasons such as hackers; unintentional mistakes because of language barriers; political reasons; and people behaviour are unpredictable. For instance, company F said *"due to political reasons sometimes"* while companies E & J said *"occasional unintentional mistakes because of [...] language (English)"* and *"cybercrime is on an increase [...] criminals constantly try to hack into the systems of financial institutions to steal money from people's accounts [...] we, as one of the financial institutions, also constantly work to protect our systems from these threats and prevent the criminals from stealing from our customers"* respectively. The language issue mentioned here means operational manuals and the technical details of a risk model in other languages other than a risk manager's first language creates some kind of uncertainties and/or result into certain risks as the two companies said. It is important to add that, the language and political issues raised here are worth noting because they illustrate different things that can post as risks to different managers in different environments. All the interviewees were Arabians and were good English communicators nonetheless the language difference could be a challenge to some of them (though only two companies mentioned it explicitly) especially with reference perhaps to the technical terms that may be contained in system documents and other related documents. Furthermore, four of the ten companies have ever experienced chain of risks, a risk from one system causing risks in other systems, due to the systems interconnectedness. These findings relate to companies' knowledge of the risk environment of their information systems and the nature of risk in each feature and that reduces uncertainties in risk management. Additionally, the companies' knowledge of the features of their information systems and especially those that pose special threats to them also influences the companies' choice of risk management strategies.

4.4 Effectiveness of Risk Management

With respect to effectiveness of risk management, ninety percent (90%) of the companies said they use tactical and systematic approaches to address risks issues. This finding shows that companies rely on both approaches to make risk management effective. Furthermore, eighty (80%) of the companies said they educate their non risks management information systems staff on risk monitoring. It is apparent that educating even the non risk management information system staff relates with the effectiveness of risk management. By educating other staff (other than the risk management staff) on risk management the companies are able to increase the effectiveness of the risk management processes such as risk identification, risk control, and risk monitoring: thus risk management becomes effective. The organizational structure that allows for the proper coordination of resources, effective communication, and team approach (that is well coordinated bottom-up and top-down approaches as well as non risk management staff and risk management staff) makes risk management effective (Schneider, Lane, and Bruton, 2009; Jones, 2010; Alberts and Dorofee, 2009).

In sum, firms attempt to increase the effectiveness of their risk management approaches can be inferred from the indication that the flexibility of the theoretical risk management model; the identification of the essential features of the information system; and the use of multiple approaches such as bottom-up and top-down to gather risk information, implement risk management actions, and for risk monitoring are important to the interviewees.

5 Conclusion and Discussion

This essay investigates into the critical factors that contribute to the effectiveness of information systems risk management in information technology projects. In addition, the impact of threats on the extent to which risk management frameworks are used and managers' perception of the effectiveness of their risk management approaches are questioned. First and foremost, the different types of critical factors such as adapting risk management approach to fit a specific risk environment; risk identification through brainstorming, cause-and-effect; organizational structures that allows for proper coordination of organizational resources and so on discussed in the literature are found to be applied many firms in risk management. It can be said that, the critical factors found in this study are related to increasing the success of risk management in general and the effectiveness of risk management models specifically. For instance, adapting a risk management model to fit different risk environments specifically increases the usefulness of the model in question and makes risk management more effective; but that means also that if any of the critical factors such as the adaptation of the model is not done properly it could lead to risk management failures. It can be noticed that the qualities of risk management models such as adaptability help companies in models selection while brainstorming, organizational structures and so on help in making risk management successful in companies. That is, critical factors underlie effective risk management from the selection of models to their application in practice.

Secondly, it is apparent that the knowledge of the essential features of an information system is important to the various managers interviewed. Companies' knowledge of the essential features of the information systems is related to the identification of the risk environment which is equally fundamental for companies to know. For instance, identifying the features is essential to risk tracking and marking out features that are difficult to manage due to the nature of their innate risk and thus help management to develop strategies to tackle the difficult risks. Furthermore, the extent to which companies' use risk management frameworks is inferred from the companies' response about their major threats. Thus threats impact on the extent of the usability of risk management frameworks.

Thirdly, the effectiveness of risk management relates to the combined efforts of both the risk management team and non risk management employees. It is apparent that managers rely on the non risk management employees to enable them to succeed in surmounting risks thus the effectiveness of risk management is achieved and/or increased. For instance, educating the non risk management staff on risk identification, monitoring and so on increases the chances of company over managing its risks successfully. That is, the effective of risk management can be inferred from the interviewees' respond using tactical and systematic approaches in addressing risk issues. Thus companies attempt to use organizational structures that facilitate proper flow of risk management information between and/or among staff to achieve effectiveness in risk management.

This study has established the importance of risk management of information systems in IT projects; it has made an interesting discovery that the reliance on risk models by companies is influenced by the ability of the models to be adjusted to render them useful in practical risk management environments and that many other critical factors underlie models' effectiveness. Furthermore, the essential features of information systems and the qualities of risk management models and their relationship or influence on effective risk management are clear in this essay. This essay confirms the relevance of the features of information system put forward by Ferris (2001) and the need for a risk management model to certify certain criteria by Alter and Sherer (2004) for effective risk management. This essay also contributes to information systems risk management in a non-Western country specifically in an Arabic country. There was no specific difference between the global companies and the Egyptian companies perhaps because all the interviewees were Arabians; however, the political and the language risks mentioned by the three interviewees illustrate default risk that companies have to deal with in some non-Western countries. The discovery made about companies depending on adaptability to select their risk management model then leads to a question if there is a causal link between the adaptable models albeit the badly managed and/or lack of risks communication proposition put forward by Bronte-Stewart (2009) and the IT projects failures. That is, the impact of adjusting risk management models to fit different risk environments in IT risk management needs further research.

List of References

Al-Shehab, Abdullah J, Hughes, Robert T and Winstanley, Graham (2005) “Modelling Risks in IS/IT Projects through Causal and Cognitive Mapping” The Electronic Journal of Information Systems Evaluation, Vol. 8, Iss. 1, pp 1-10, available online at www.ejise.com
Alberts, J. A. C. & Dorofee, J. D. A. (2009) A Framework for Categorizing Key Drivers of Risk, Carnegie Mellon University/Software Engineering Institute (CMU/SEI)-Technical Report (TR)-007

Applegate, M. L., Austin, D. R., and McFarlan, W. F. (2007) Corporate Information Strategy and Management: Text and Cases, 7th Edition, United States: McGraw Hill

Apostol-Maurer, I. (2008) Optimization Alternatives of Information Systems for Risk Management, Revista Informaticã nr. 3(47)

Alter, S. and Sherer, A. S. (2004) A General, But Readily Adaptable Model of Information System Risk, Communication of the Association for Information Systems (Vol. 14, 2004), pp.1-28

Association of Insurance and Risk Managers (AIRMAC), The Institute of Risk Management (IRM), & ALARM (2002) A Risk Management Standard, http://www.theirm.org/publications/documents/Risk_Management_Standard_030820.pdf Accessed on (2011-03-06)

Anonymous (n.d.) The History of Information Systems in Business
http://www.uwosh.edu/faculty_staff/wresch/311IShistory.htm Accessed on (2011-03-03)

Anonymous (n.d.) What is Research Design? http://www.nyu.edu/classes/bkg/methods/005847ch1.pdf Accessed on (2011-03-11)

Argyris, C., & Schön, D. A. (1978). Organizational learning II. Reading, MA: Addison-Wesley

Belle, V. J., Eccles, M., and Nash, J. (2003) Discovering Information Systems, California: Creative Commons

Beynon-Davies, P. (2009) The ‘Language’ of Informatics: The Nature of Information Systems, International Journal of Information Management, Vol. 29, pp.92-103

Bolfíková, E., Hrevova, D., and Frenova, J. (2010) Manager’s Decision-making in Organizations: Empirical Analysis of Bureaucratic vs. Learning Approach, Zb. rad. Ekon. fak. Rij. • vol. 28 • sv. 1 • 135-163

Bronte-Stewart, M. (2009) Risk Estimation from Technology Project Failure, 4th European Conference on Management of Technology, 6-8 September, Glasgow-Scotland

Buehring, S. (2009) Risk Management Principles: How to Identify and Deal with Risks, Project Smart

Cule, P., Schmidt, R., Lyytinen, K., & Keil, M. (2000). Strategies for heading off IS project failure. *Information Systems Management, Vol. 17, No.*2, 65–73.

ExecutiveBrief (2008) Ranking Risks: Rare to Certain, Negligible to Catastrophic, Project Smart

Eric, S., Keven, G.R., & Jerrold, M.P. (n.d.) The Insider Threat to Information System: The Psychology of the Dangerous Insider, Reprinted from Security Awareness Bulletin, No. 2-98 http://www.pol-psych.com/sab.pdf Accessed on (2011-03-05)

Ferris, J. (2001) An Investigation and Analysis of Risk Models and the Creation of a New Framework for IT Investment Risks and Models for Risk Management, Proc. Satisfying the Customer, Escom, London

Gill, J. and Johnson, P., (2002), Research Methods for Managers, 3rd, Sage Publishing, London

Golafshani, N. (2003). Understanding reliability and validity in qualitative research.
The Qualitative Report, 8(4), 597-606. Retrieved [2011-03-11], from http://www.nova.edu/ssss/QR/QR8-4/golafshani.pdf

Hazel, T. (2006) Risk Management and Problem Resolution Strategies For IT Projects: Prescription and Practice, Project Management Institute, Vol.37, No. 5, pp.49-63

Hinkin, T. R. (1995) A Review of Scale Development Practices in the Study of Organizations, Journal of Management, Vol. 21, No. 5, 967-988 Copyrighted in 2001

Hillson, D. (2010) Managing Project Risk: What's New?
http://www.executivebrief.com/risk-management/managing-project-risk/ Accessed in January 2011.

Huseyin, C., Birendra, M., and Srinivasan, R. (2005) *The Value of Intrusion Detection Systems in Information Technology Security Architecture*
Information Systems Research 16(1), pp. 28–46, ©2005 INFORMS

Hedman, J. and Kalling, T. (2002) IT and Business Models: Concepts and Theories, Sweden: Liber AB

Issa-Salwe, M. A. & Ahmed, M. (2011) Risk Management of an Information System by Assessing Threat, Vulnerability and Countermeasure, International Journal of Research and Reviews in Computer Science (IJRRCS) Vol. 2, No. 1, pp.111-114

James, T. (2003) Managing Information Technology Projects: Applying Project Management Strategies to Software, Hardware, and Integration Initiatives, New York, NY, USA: AMACOM, pp. 152-182

John, M. & Trevor, W-H. (2007) "Understanding the Sources of Information Systems Project Failure". Management Services. FindArticles.com.

http://findarticles.com/p/articles/mi_qa5428/is_200710/ai_n21295900/ Accessed on (05 Mar, 2011)

Jones, G. (2010) Organizational Theory, Design and Change, 6th Edition, New Jersey: Pearson Education, Inc., pp.29 & 276-277

Jutte, B. (2010) 10 Golden Rules of Risk Management, Project Smart

Keil, M., Cule, P., Lyytinen, K., & Schmidt, R. (1998). A framework for identifying software project risks.*Communications of the ACM, Vol.4, No.*11, 76–83.

Kloman, H. F. (1990) "Risk Management Agonists." Risk Analysis 10, 2 (June 1990): 201-205.

Knupfer, N. N. & McLellan, H. (1996). Descriptive research methodologies. In D. H. Jonassen (Ed.), *Handbook of research for educational communications and technology* (pp. 1196-1212). New York: Macmillan

Maxwell, J. (1997). Designing a qualitative study. In L. Bickman & D. J. Rog (Eds.) Handbook of applied social research methods (pp. 69-100). Thousand Oaks, CA: Sage.

Miller, J. M. (n.d.) Graduate Research Methods: RE8 600, Western International University

NetworkWorld (n.d.) Defending Against the Insider Threat, Jupiter Networks http://www.juniper.net/us/en/local/pdf/whitepapers/defending-against-the-insider-threat-nw.pdf Accessed on (2011-03-05)

Olzak, T. (2008) A Practical Approach to Managing Information Systems, Erudio Security, LLC

Pathirage, C.P., Amarantunga, R.D.G and Haigh, R.P. (2008) The Role of Philosophical Context in the Development of Theory: Towards Methodological Pluralism, The Built & Human Environment Review, Volume 1, pp.1-10

PricewaterhouseCoopers LLP (2004) Enterprise Risk Management: Integrated Framework (Executive Summary) in Committee of Sponsoring Organizations of the Treadway Commission-COSO

Radack, S. (2009) Risk Management Framework: Helping Organizations Implement Effective Information Security Programs, United States: NIST

Randall, C. R. and Arthur, H. G. Jr., (2009) Monitoring Risk in Information Technology Projects in Allied Academies International Conference: Academy of Information and Management Sciences Proceedings, Volume 13, Number 1, pp.58-62

Ridley, K. (2005). The Multimedia Activity Recall for Children and Adolescents (MARCA): Development and Validation. PhD thesis, University of South

Australia, School of Health Sciences, pp. 60-67.

Ralph, S., George, R., and George, W. R. (2010) “Principals of Information Systems” 9th Edition, Cengage Learning http://www.google.com/books?hl=sv&lr=&id=TlQCvdWQkfEC&oi=fnd&pg=PR24&dq=Concepts+of+Information+Systems+Risk&ots=t4R28XQpVw&sig=29EUOjGUO63m3Gxw9i-32AZmeLk#v=onepage&q=Concepts%20of%20Information%20Systems%20Risk&f=false Accessed on (2011-03-06)

Schneider, P. G., Lane, S., and Bruton, M. C. (2009) Monitoring Risk in Information Technology Projects in Allied Academies International Conference: Academy of Information and Management Sciences Proceedings, Volume 13, Number 1, pp.63-65

Sauer, C., and Cuthbertson, C. (2003) “The state of IT project management in the UK.” Templeton College, Oxford University.

Schlaak, B., Scott, D., Lutz, M. K., and Ragnar, S. (2008) Managing of Information Systems Risks in Extended Enterprises: The Case of Outsourcing, Proceedings of the Fourteenth Americas Conference on Information Systems, Toronto, ON, Canada August 14th-17th 2008

Shirley, G. (2006) The Nature of Theories in Information Systems, Management Information Systems Quarterly

Standish Group (2001). Chaos chronicles II. West Yarmouth, MA

Standish Group (2003) “CHAOS Chronicles report”, Yarmouth, MA

Sherer, A. S. and Alter, S. (2004) Information Systems Risks and Risk Factors: Are they mostly about Information Systems, Communication of the Association for Information Systems (Vol. 14, 2004), pp.29-64

Symantec Corporation (2007) IT Risk Management Report: Trends through December 2006, Volume 1

Symantec Corporation (2008) IT Risks Management Report 2: Myths and Realities

Shaker, K. (2010) The Seven Deadly Sins of Risk Management, Project Smart

Tiwana, A. and Keil, M. (2004) The One-Minute Risk Assessment Tool, Communication of the ACM, Vol. 47, No. 11, pp.73-77

Walsham, G. (1995) The Emergence of Interpretivism in IS Research, Information Systems Research 6(4), pp.367-394, Copyrighted in 2001

Wrona, V. (2008) Your Risk Management Process: A Practical and Effective Approach, Project Smart

Yusuff, N. Y. M. (n.d.) Contemporary Approaches to Project Risk Management: Assessment & Recommendations http://www.infosecwriters.com/text_resources/pdf/IS_Project_Risk_Mgmt.pdf Accessed on (2011-03-06)

Appendix I: Structured Interview Questions

Structured Interview Questions by Ahmed Abd Elkhalek

This interview is intended to get your input into a Master thesis I am writing on Information Systems risk management as part of the requirement to complete a master program on IT Management at Mälardalen University.

The input obtained from you in this interview is intended solely for this project and will not under any circumstances be transferred to any other project and/or person.

Your confidentiality is assured. Thank you for your understanding.

I. **Information Systems Risk Management**

1. Do you have a risk management model?

2. What is the name of your company's risk management model?

3. Which one of the following best fit the description of your risk management model?

A. Theoretical risk models

B. Company's own risk models

C. Other……………………

4. Do you interact with all your workers perhaps in a form of discussion group about risk management?

A. Yes

B. No

5. If yes, how often? If no, why?

A. More

B. Less

C. Other, please specify……………………………………………………………

6. Which of the following are essential processes in your risks management?

A. Risk Identification

B. Risk Assessment

C. Risk Controlling

D. Risk Monitoring

E. Other: Please specify ……………………………………..

7. Which of the following technique (s) best fit the way your company gathers information relevant to information systems risk management?

A. Questionnaires to the system actors (technical and nontechnical workers involve in the information systems)
B. On-site interviews
C. Periodic Brainstorming
D. Document Reviews: Policy documents, system documents such as system user guide
E. Use of Automated Scanning tools: A technical tool for the collection of information relevant to information systems
F. Workers are encouraged to report any suspected threats at anytime
G. Other: Please, specify……………………………………..

8. Which of the following fit the description of your company's method of risk assessment?
A. Cause-and-effect
B. Risk matrix
C. Both
D. Other: Please, specify………………

9. Which of the following countermeasures to you have in place for risks control?
A. Our organizational structure allows for effective communications and use of resources that lessens risks
B. We have technology that monitors and manages the performance of our systems
C. We have a comprehensive insurance on our information systems
D. Other………………………………………………………………………..

10. Do you have risk cues in place for monitoring of risks?
A. Yes
B. No

II. Qualities of Risk Management Model

11. Which one of the following do you attribute to the criteria your company used to choose its risk management model?
A. Clarity
B. Practicality of use
C. Completeness
D. Adaptability
E. All the four above
F. Other: Please, specify……………………………….

12. Which one of the attributes in 11 above do you like most about your risk management model? Why?

III. Features of Information Systems

13. From your company’s perspective, which of the following are essential features of its information systems?

A. Technology

B. Information

C. People

D. System-Hardware and software

E. Other…………………………….

14. Which one of the features mentioned in 13 above will you consider difficult to manage in terms of its innate risks?

15. What makes it particularly difficult to manage?

16. Which one of the following broad factors poses a greater threat to your company’s information systems? Please, provide percentages, if possible, to match with the levels of their threats.

A. Technical Factors: Example Human Threats-Human actions both intentional and unintentional such as insider threats and malicious attacks

B. Nontechnical Factors: Example Natural Threats such as Extreme temperatures

17. Please, briefly explain the reason for your choice in 16) above.

18. Have you ever experienced the “Domino Effect: a chain of causation where a risk from one feature causes another risk in another feature and/or risk from a technical (or nontechnical) factor causes another in the other factor”?

IV. Effectiveness and Efficiency of Risks Management

19. Which of the following describes how your company addresses risks?

A. Tactical approach: Workers working on tasks are encouraged to be alert for risk and once identified separate statements are issued for each risk.

B. Systematic approach: It is the task of top management to work on everything concerning risk

C. Both

D. Other………………………………………………………………………………

20. Do you give your information systems staff (those who are not associated with risk management) some basic education on monitoring risk?

A. Yes

B. No

Thank you for your time and invaluable input.