RISK MANAGEMENT AND ELECTRONIC RISK INCORPORATION WITHIN MODERN ORGANIZATION

Dr. Amine Nehari Talet
King Fahd University of petroleum &
Minerals, Saudi Arabia
nehari@kfupm.edu.sa

Abstract

Fast growth of the information technology revolution, the prevailing economic crisis and hasty changes in business environment organizations the World Wide Web has become very necessary for building efficient and effective electronic business. Risk management and electronic risk is becoming a key factor within modern organizations since it ensures a successful execution of projects. Due to this fact, information flows and process structure must be managed carefully to reduce risks that might face the progress of projects. This paper will present most type of risk that might affect E-businesses and Risk sources. It will suggest a Guideline that any organization can consider in its plan that will be useful while dealing with these risks before and after they occur.

Key words: Risk, Risk Management, Electronic Risk, Electronic Risk Identification, Virus Risk, and Internet Risk.

1. Introduction:

Risk is the possibility of something going wrong as consequence of a threat or a vulnerability which can have a major impact on the operation (Mees, 2007). Additionally, Most companies have introduced security measures to protect their computer systems; many had not sought to safeguard against liability exposures, including computer fraud, privacy violations. Businesses have changed dramatically over the last decade. The pervasiveness of technology and, more recently, than advent of the internet have resulted in businesses becoming reliant on the effectiveness of their IT systems. While this has resulted in great rewards in terms of efficiency and productivity, many problems can plague a software project.

RM is described as a systematic and iterative process of identifying, analyzing, and responding to project risks in order to reduce the potential negative events and maximizing the positive events in terms of consequences and probabilities (Kasap D. & Kaymak, 2007). Also, Pressman (2005) describe Risk management is concerned with identifying risks; understand risks and drawing up plans to minimize their effect on project. Risk management is series of steps that help a team to understand and manage uncertainty.

A risk is potential problem, it might be happen or it might not. But regardless of the outcome, its good idea to identify it, assess its probability of occurrence, estimate its impact, and establish a contingency plan should the problem actually occur. Jaafari

(2001) explain the risk can be expressed mathematically as the probability of occurrence of loss gain multiplied by its respective magnitude.
Antia (2001) describe electronic commerce transactions by reaching a worldwide audience at very low cost by using the Internet. Using the Internet poses different sorts of trust problems which businesses must take it into consideration to minimize risks. When the customers are confident about the security of their personal information, such as financial data and credit card number, they submit their information and purchase goods or services via the Web. David(2001) identify E-risk is any risk that yield from the use of new electronic technology, especially from the use of computer, telecommunications and the Internet.

George (2000) defined information technology related risk as the likelihood that an organization will experience a significant negative effect in the course of acquiring, deploying and using information technology either internally or externally.

The rest of this paper is organized as follow. Section (2) introduces Review of related studies. Section (3) present E-Risk Frameworks include introduces related E-Risk Source in general, outlines E Risk Management Process and Technology Guideline for Managing E-risk.

2- Introduces Review of Related Studies:

In this section The researcher investigate a various study related in E-Risk source and E-Risks Process, Such asA structure designed by Cornford (1998) described risk management process into risk identification which results in variety of technological content, environmental communications, the execution and operation approaches, programmatic constraints and the mission duration. The second is Risk Analysis of the consequences of the possible risks by scoring their impact on the necessities should they occur. The result is a requirement-driven risk list where failures are listed based on their impact on weighted requirements. Risk planning phase has the following design rules, process controls, testing, modeling, and inheritance). Risk Tracking contains a tool to display the number of report formats to be used by different personnel for different reasons. Risk Control is designed for implementation. This allows the project team to effectively control risk and watch its growth or decline as the design evolves and the results of implementation become available.

A framework proposed by Jurison, (1999) described the risk assessment in three steps; the first one is risk Identification, which is purposed to develop a list of risks that can adversely impact project outcome. The second step is risk analysis, which is intended to assess the risk exposure, the likelihood and impact of each risk and the final step is the risk prioritization, which is used to produce a list of risks prioritized by the impact.

Smith and Merritt, (2002) claimed that risk management process contains the following phases: identifying risks using brainstorming techniques to discover any risks that forbid the progress of the project, analyzing risks by the team to determine if a certain risk is worth migrating or not, prioritizing and mapping risk to establish a the seriousness of the risk according to their impact, and resolving risks by implementing plans to prevent risk from occurring.

Sommerville, (2001) Stated that risk management involves the following stages: 1) Risk identification 2) Risk analysis 3) Risk planning 4) Risk monitoring. [1] acknowledged that the risk management process involves 1) Risk identification, which entails checklist, questionnaires or brainstorming meeting 2) Risk analysis to assess the identified risk in order to create a contingency measures to decrease the risk impact and 3) Risk monitoring to guarantee the effectiveness of the methods followed.

Vaidyanathan and Devaraj (2003) show the five sources of New Online Risks, The new online risks may be attributed to the following five functions that have emerged for online B2B business: new services, new business models, new processes, new technologies, and new fulfillment needs. Each of these five functions plays an important role in this framework. New services: The rise of the e-business has changed the way that many organizations function and exist.

New business models: New business models have emerged on the online scene. Portal models such as dynamic pricing, free products and services, demand-sensitive pricing, and so on. Products and services have made their way to the e-business to be sold by original manufacturers, certified resellers, and sometimes no certified resellers as well. The original manufacturer or service provider may find it attractive to channel their marketing and sales efforts using e-marketplaces or exchanges, only to find that the owners of the e-marketplaces or exchanges have different business models than their conventional marketing and sales practices. When the business models of the original manufacturer are not aligned with the certified resellers or non-certified resellers, the original manufacturers will be exposed to various new risks.

New processes: New e-business processes have surfaced to fill a real business need. Companies that have emerged onto the online scene have changed the old processes to build new business models. Integration of external partner process with internal process has created new reengineered processes. These new processes may expose new risks. The creation of real-time process for e-business may also expose new risks. New outsourcing processes may also create risks for the business. New technology: E-business uses emerging technologies. Most of these technology applications may not have been tested for scalability, security, and availability. The integration with other software products has also been a challenge. Integration of various systems and software has exposed the integrated system’s vulnerabilities, these vulnerabilities may highlight unique risks caused specifically by integration (Kolluru and Meredith, 2001) (Salisbury 2001).

New fulfillment: The perception of online fulfillment has changed. Products and services are needed almost in real-time in this online world. E-business may bring in sales from many directions. The integration of these real-time sales orders with the existing supply chain management and order fulfillment may expose risks. Inefficient fulfillment integration with external distribution providers may also expose risks (Papadopoulou 2001).

Another study by Tan and Guo (2005) show the risks of the online transactions, these risks can come from many aspects, such as the privacy issues, e-commerce technology, lack of reliability in e-commerce processes, the lack of the social, financial and legal infrastructures of the e-commerce environment. Pichler (2000) presented a wide range of technologies and strategies, such as privacy, security, and reputation systems attempt to depress these risks.

Nancy (2004) Explain the risk face the employers whom used email and instant messaging it shows the most effective way to reduce e-mail and instant messaging risk like, Establish written policies that clearly spell out the rules governing employee e-mail and instant messaging use and the need for strict compliance and Enforce your policy with a combination of disciplinary action and software that monitors and filters e-mail and instant messaging content in conjunction with written policy.

Managing risk by Beck et al (2002) describe four phases. The first phase Risk Identification the process of identifying the threats of the business. The threats according to security taxonomy are Strategic risks, Operational and Systems risks; Legal and Regulatory risks; and financial risks. Second phase Risk Evaluation refer to producing a list of all possible threats to the e-business in relation to like hood and their severity. Third phase Risk Control is decided in which the best suitable and cost-effective measures need to be executed to control the risks. Such measures can involve: Risk avoidance; Risk reduction; and Risk transfer and fourth phase Risk monitoring provides a review of the organization's ability to deal with incidents that might result in business interruption.

Sommerville, (2006) stated that RM involves the following stages: 1) Risk identification, which entails checklist, questionnaires or brainstorming meeting. 2) Risk analysis to assess the identified risk in order to create a contingency measures to decrease the risk impact, and 3) Risk monitoring to guarantee the effectiveness of the methods followed. Figure 9 illustrates the RM process.

Parker (2007) explain the increasing information security losses Information technology trade publications report increasing information security losses, questionable risk management and risk assessments, and under funding and understaffing. Government departments receive low grades in security. Legislators react by adopting draconian laws such as Sarbanes-Oxley. The poor state of information security derives from a fundamental risk-based approach to security. A security risk is defined to be an adversity, but measuring security risk requires anticipating frequency and impact of rare loss events in a specific security setting. Security risk is different than measurable business risk that consists of voluntarily investing resources to produce a profit or meet a goal. Security risk is not measurable, because the frequencies and impacts of future incidents are mutually dependent variables with unknown mutual dependency under control of unknown and often irrational enemies with unknown skills, knowledge, resources, authority, motives, and objectives—operating from unknown locations at unknown future times with the possible intent ofattacking known but untreated vulnerabilities and vulnerabilities that are known to the attackers but unknown to the defenders (a constant problem in our technologically complex environments). In addition, when enemies cannot exploit one vulnerability, they often attack other vulnerabilities to accomplish their goals. Therefore, risks arerelated in unknown complex ways so that reducing one risk may increase or decrease other risks. Also, the impact may be minimal in major attacks and major in minorattacks.

3- Proposed E-Risk Framework:

In this part we will start by describing the component of the Proposed E-Risk framework, see model 1.this Model Include three parts: first part is the E-risk sources divided in four type :Viruses Risks, Internet Risks, E-Business Risks and E-mail Risk. Second part describes the E-risk Management Process, and the final part explains the guideline for managing E-risk.

3.1 E-Risk Sources:

There are many types of E-Risk, in the next paragraph I will talk about some of them.

3.1.1Viruses Risks:

A computer virus is contagious; it replicates itself and infects a computer, which has contact to the others computer by networks or by different types of disks.

3.1.2 Internet Risks:

The Internet is a global computer connection system that allows rapid and broad communication. With any new method of communication, there are risks as well as benefits. Persons who communicate over the Internet should consider these risks carefully: Loss of Information Control, data Privacy, and data integrity.

The Loss of Information Control which Internet increase the risks associated with information: free accessibility, interactivity, and connectivity of personal, economical, political, media communication and services are used by authorized person in an uncontrolled way have all led to a loss of information control. Loss of Data Privacy the Internet is not private. Message can be copied and forwarded to one or a million people with only a few keystrokes by the person who receives your message. Loss of Data Integrity Which means information is created, modified, or deleted by an intruder.

2.1.3 E-Business Risks:

Electronic business is the conduct of business with the assistance of telecommunications and telecommunications-based tools. The Risk such as the failure of software may be due to viruses and failure of network and computer hardware.

3.1.4 E-Mail Risks :

Many of the risks to e-mail are not new and are similar to those associated with post office mail, faxes or voice mail. The scale of e-mail risks is greater than any other existing communication medium, because technology makes changing and redirecting e-mail effortless.

3.2 E-risk Management Process:

E-Risk Management is very important aspect which mean that you can anticipate what might be occur and how to deal with it. Ward and Chapman (1994) identify the purpose of risk management is to reduce or neutralize potential risks, and simultaneously offer opportunities for positive improvement in performance. Risk may threaten the project, the software that is being developed or the organization. The general approach to risk management is that it is a three-tiered process that consists of the identification of risks, their evaluation or assessment, and finally a procedure for dealing with them (Smith et al. 2001). The researchers identify four stages of E- Risk Management:

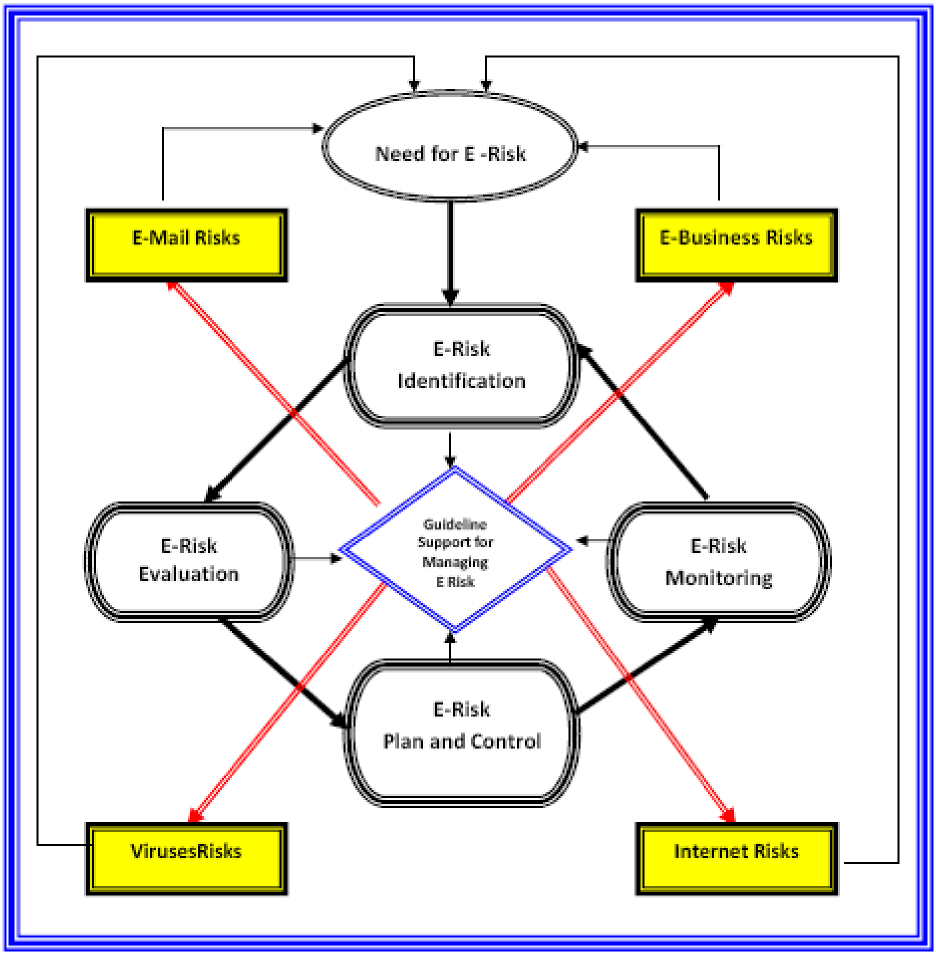
In this conceptual framework, the first stage is the need for E- risk management which addresses the necessity for the organization to implement risk management processes. The organization must explicitly define the importance of risk management to their stakeholders to contribute in identifying all risks associated with business objectives. Identifying all relevant stakeholders is essential for the success of the risk mitigation process (Kontio, 1998). These risks may be obstacles for the organization in achieving the stated business objectives. When an organization plans a new business strategy, it must identify all risks associated with it in order to mitigate the obstacles and to facilitate the implementation of the new strategy in terms of the goals. Risk management is needed in day to- day business operations and project management implementation. Understanding the need of the risk management is vital for success of organization existence in dynamic world. The need will establish the goal definition for implementing the risk management.

The second stage is E-Risk Identification means the undertaking of a comprehensive identification of the threats. Beck et al (2002) describe Failures in technology or network security, which can expose the company to fraudulent activities, Problems in adjusting the company’s business processes to the demands of e-commerce, Interruption to the business operation, with the likely consequence of reputation damage, is of particular concern to the online business, Uncertainty over international legal rules, And Electronic payments risks. This phase will produce a list of all risks associated with any project.

The third stage E-Risk Evaluation include identified risk is considered in turn and a judgment made about the probability and the seriousness of the risk, it depends on experience of the project manager.

The fourth stage E-Risk Plan and Control in this phase the decisions require to be taken as to the most appropriate and cost effective measures that might be implemented in order to control the risks. The planning stage provides different execution possibilities and examines different What-if options (Cornford el al 2001).

The final phase E-Risk Monitoring means that assessing each of the identified risks to decide whether or not that risk is becoming more or less probable. Cano and Cruz (2002) stated the risk monitoring must deal with risk evolution such as factors, triggers and responses.



Proposed Model (1)

Conceptual Framework for Managing Electronic Risk

3.3 Technology Guideline for Managing E-risk:

An effective technology guideline must consider a lot of things for managing E-Risk; we will talk about major issue such that Infrastructure, Security, Privacy, Business Processes, Services, Management, Content, and Management Information. Best practices for dealing with electronic risk as follows:

Managing Technology infrastructure: consist of Development, Protection, and Maintenance of databases, Server/Database availability and scalability, 24 / 7 network and system monitoring.

Managing Security: include Intrusion detection, Fraud Detection, and Assessment of application-level security to control access.

Privacy: take in Prevention of unauthorized access, Protection of all internal and external Web-based communications, Compliance with international law and trade agreement for multinational companies.

Business Processes: contain Maintaining transaction and payment integrity, Monitoring and management of e-mail communications, Identifying and managing electronic vital records.

Services: consist of Software availability and download via the internet, providing Internet access for the enterprise and third parties, and Management of internal and external service-level agreement.

Management: include Management processes for standardizing and controlling business conducted over the internet, formally documented plan/procedures to handle electronic evidence, and ongoing maintenance of corporate e-risk, including awareness and education.

Content suggested Creation and management of multimedia content, Management of content-based electronic record, and Procedures for detecting and handling errors in Web content and incorrect/broken links.

Management Information: takes in Capturing, aggregating, reporting operational statistics for performance monitoring, trend analysis, and capacity planning, and Transactional analysis for fraud detection.

4- Conclusion:

This paper Incorporating Risk Management and Electronic Risk as Conceptual Framework, The objectives of this paper provides valuable guidance to managers seeking to reduce risk when used the internet. In fact, the user of new technology is expected to encounter the following problems, Viruses, risks, Business Risk, E-mail and Internet risks. These four problems are highly related to each other and may lead to great problems when used the internet.

Based on the topic of this research, this paper concluded that the proposed Risk Management and Electronic Risk as Conceptual Framework would give a broadest analysis of the E-risk management process, Methods for managing the risk in each of these categories have been suggested, and also, a conceptual technology guideline is suggested for managing E-Risk.

References:

Blackburn, Steven C. (1999) Managing the Risks of the Internet. *Rural Telecommunications*, Vol. 18 Issue 5, p56, 3p.

Beck, Mattthias.Drennan, Lynn. Higgins, Adrian. (2002) Managing E-Risk.. *Association of British Insurers*

Cano, A. Cruz, P (2002) Integrated Methodology for Project Risk Management. *Journal of Construction Engineering and Management.*

Cornford, S. Feather, M. Hicks, K. (2001) Tool for life-Cycle Risk Management. Jet Propulsion Laboratory, CalifornaiaInstitutte of Technology.

Cornford, S. "Managing Risk as a Resource using the Defect Detection and Prevention process," International Conference on Probabilistic Safety Assessment and Management, 1998, pp.13-18.

Donn B. Parker. (2007) inside risks: Risks of risk-based security, *Communications of the ACM*, Vol. 50 Issue .3.

Dodson, George. (2000) E-business Impact on IT Management. *Candle Computer Report*. Vol. 22 No.3.

Flynn, Nancy. (2004)E-Risk Factor' Vol. 64 Issue 8, pp21-22.http://search.ebscohost.com/login.aspx?direct=true&db=buh&AN=15421948&site=ehost-live

Ganesh Vaidyanathan, SarvDevaraj. (2003) Virtual extension: A five-factor framework for analyzing online risks in businesses, *communications of the ACM*, Vol. 46 Issue .12.

Haixia Tan, JianfengGuo. (2005) E-marketing & e-businesses: Some methods to depress the risks of the online transactions, *Proceedings of the 7th international conference on Electronic commerce ICEC*.

Jaafari, A. (2001) Management of Risks, Uncertainties and Opportunities on Projects: Time for a Fundamental Shift. *International Journal of Project Management* Vol.19 No.2 pp 89-101.

Jurison, J. "Software Project Management: A Manager's View, " Communications of AIS (2:17), 1999.

Kolluru, R and Meredith, P. (2001) Security and trust management in supply chains.*Information Management and Computer Security*.Vol .9 No.5, pp 233–236.

Kontio, J., Getto, G., and Landes, D. "Experiences in improving Risk Management Processes using the concepts of the Riskit Method," In Proceedings of the ACM SIGSOFT 6th international symposium on Foundations of software engineering ACM Press, New York, 1998, pp.163-174.

Kasap D., &Kaymak, M. (2007). Risk Identification Step of the Project Risk Management Management of Engineering and Technology Paper presented at the Portland International Center for Portland, Oregon, USA.

Matthias Beck, Lynn Drennan and Adrian Higgins.(2002) Managing E-Risk, *Published by the Association of British Insurers*.

Mees, W. (2007). Risk Management in Coalition Networks. Third International Symposium on Information Assurance and Security, pp 329-336.

Salisbury, W .(2001) Perceived security and World Wide Web purchase intention, *Industrial Management and Data Systems* .Vol.101, No4, pp165-176.

Smith H. A., McKeen J. D., Staples D. S. (2001). Risk Management in Information Systems: Problems and Potentials. *Communications of the Association for Information Systems.*

Smith, P.G., and Merritt, G.M. "Proactive Risk Management: Controlling Uncertainty in product Development, " 2002, New York: productivity press.

Sommerville, I. Software Engineering, 6(Edition), 2001, pp. 84-85.

Papadopoulou, P (2001) Trust and relationship building in electronic business. *Electronic Business Research: Electronic Networking Applications and Policy*. Vo.l11 No. 4, pp322–332.

Pressman, Roger. (2005) Software Engineering practitioners approach 6 Edition. Chapter 25 pp 726

Pennathur, Antia. (2001) 'Click and brick' E-risk management for banks in the age of the, internet, *Journal of Banking & Finance*, Vol. 25 Issue 11, p2103, 21p.

Pichler, R. (2000) Trust and Reliance Enforcement and Compliance: Enhancing Consumer Confidence in the Electronic Marketplace. *Stanford Law School.*

Ward, S., and Chapman, C (1994) Transforming Project Risk Management into Project Uncertainty Management.*International Journal of Project Management* Vol. 21No.2, pp 97-105

Wollf, David. Gasper, Juli-Ann. (2001)Transaction of risk Management by Technology Creighton University.

1. CEPII, la compétitivité des nations 1999.
2. LichèleDebonneuil et Lionel Fontagne « compétitivité », rapport du conseil d'Analyse Economique, 2003.
3. Lean-Louis MUCHIELLI, « la compétitivité : définitions, indicateurs et déterminants »
4. La compétitivité des nations selon le Forum Économique Mondial - Rapport 2010/2011
5. Ahmed touil « Eléments d'analyse de l'impact de la libéralisation commerciale sur la dynamique de l'emploi : le cas algérien », les cahiers du MECAS, 2007.
6. Ahmed touil, ouvrage déjà cité.
7. Rapport FMI 2005.
8. Jean- Pierre Cling « commerce, croissance, pauvreté et inégalités dans les PED : une revue de littérature », DIAL, 2006.
9. S.Dupush, E.M. Mouhoud et F.Talahite, « les perspectives d'intégration entre l'Union européenne, les PECO et les pays sud méditerranéens : incidences sur les tendances de la spécialisation des activités en Europe », février 2003
10. Il prend des valeurs comprises entre 0 pour une spécialisation nulle et 2 pour une spécialisation complète.
11. S.Dupush, E.M. Mouhoud et F.Talahite, « les perspectives d'intégration entre l'Union européenne, les PECO et les pays sud méditerranéens : incidences sur les tendances de la spécialisation des activités en Europe », février 2003
12. S.Dupush, E.M. Mouhoud et F.Talahite, ouvrage déjà cité
13. KassimBouhou « l'Algérie des réformes économiques : un gout d'inachevé », politique étrangère 2-2009.
14. Le quotidien algérien El Watan, le 24 aout 2008.
15. La banque mondiale 2008.
16. WORLD ECONOMIC FORUM, la compétitivité en Afrique 2009.
17. WORLD ECONOMIC FORUM, la compétitivité en Afrique 2009.
18. www.lexpertjournal.com