Risk Mitigation and Monitoring Strategies for Financial Information Systems

Ann Kibe*,Prof Waweru Mwangi ,Dr Stephen Kimani
School of Computing and IT, Jomo Kenyatta University of Agriculture and Technology, P O Box 62000-00200 Nairobi Kenya
* E-mail of the corresponding author: anncax@gmail.com

Abstract
Risk is a concept that denotes a potential negative impact to an asset or some characteristic of value that may arise from some present process or future event. In everyday usage, risk is often used synonymously with the probability of a known loss. Risk management can be defined as the human activity which integrates recognition of risk, risk assessment, developing strategies to manage it and mitigation of risk using managerial resources. The strategies include transferring the risk to another party, avoiding the risk, reducing the negative effect of the risk and accepting some or all of the consequences of a particular risk. The objective of risk management is to reduce different risks related to a pre-selected domain to a level accepted by society.

Risk management is the process that allows managers to balance the operational and economic costs of protective measures and achieve gains in mission capability by protecting the Information systems and data that support their institution' missions. This process is not unique to the IT environment; indeed it pervades decision-making in all areas of our daily lives. The head of an organizational unit must ensure that the organization has the capabilities needed to accomplish its mission. These mission owners must determine the security capabilities that their Information systems must have to provide the desired level of mission support in the face of real-world threats. A well-structured risk management methodology, when used effectively, can help management identify appropriate controls for providing the mission-essential security capabilities.

This paper explores various strategies and options for mitigating and monitoring risks facing financial information systems in performing risk management of financial information systems in order to minimize the losses incurred when faced by the various risks.

Keywords: Riks, risk mitigation, Risk management, Risk monitoring

1.1 Introduction

Information Communication Technology (ICT) has become an attractive means of improving the process of gathering information (Soliman and Janz, 2011). ICT systems now typically facilitate effective operational control within all functions in financial institutions, support the financial institution's strategic planning and decision making, as well as increasingly help in managing the financial institution's interface with its customers, suppliers and financial partners. There are different kinds of information systems for various financial institution functions. These include Human Resource Information Systems, Accounting Information Systems, Expert Information Systems, Enterprise Resource Planning Systems, Planning Support Information Systems and Marketing Information Systems.

The importance of Information Systems (IS) for the operation of financial institution nowadays is widely recognized, while security is one of the major concerns of IS management. A commonly used security management methodology is risk management, which is recommended by The International Standards Organization (ISO) (ISO/IEC, 2005), while The Computer Security Institute (CSI) (2005) emphasizes that risk management aspects of computer security have become important concerns to today's financial institution. It is also recognized that risk management is affected by organizational elements, including social and cultural aspects (Karyda et al., 2011).

Whitman et al. (2007) points out that while some security issues may be common to most financial institution, others are "idiosyncratic to individual financial institution or industry groups". Thus, there is not one security solution that is suitable for all financial institution. Perhaps the major problem facing researchers and managers in the area of risk is that risk is itself an abstract concept (Gerber and von Solms, 2005). While hazards and their aftermath can be identified, risk depends on a complex interplay of a number of social variables, which are ultimately combined by human judgment.

1.2 Risks Faced in Applying Information Systems in the Financial Institutions

A number of models for understanding IS failures have emerged. One study examines failure in terms of ignoring a number of organisational behaviour factors arguing for the importance of organisational variables. Lyytinen and Hirschheim's (2005) comprehensive study has mapped the following concepts of IS failure:

Correspondence failure: The IS fails to meet its design objectives;

Interaction failure: The users maintain low or non-interaction with the IS;

Process failure: The IS overruns its budget or time constraints; and

Expectation failure: The IS does not meet stakeholders' expectations.

To these types Sauer (2009) adds *Termination failure* (systems outage), when developmental or operational activities stop, leading to stakeholders' dissatisfaction due to the limited provision of service by the IS.

Correspondence failure arises when the IS function deployed as a decision support system fails to provide management with the right information. Despite the information overload available, what managers need is relevant information and thus, IS that are designed to distil information and only feed managers with what they need to make effective decisions. Apart from expectation and termination failure concepts, the other types adopt a highly rational view of IS failure that is limited in capturing the complexity of the phenomenon. However, these types of failure are useful in showing surface manifestations of deeper organisational pathologies (Goulielmos, 2010).

Other reasons cited for IS failure include a lack of strategic direction given by the business to IS investment decisions, often reflected in a misalignment between IS strategy and processes on the one hand and business strategy and processes on the other; inability to leverage existing ICT infrastructures (to the financial institution function); 'paving the cow paths' rather than capitalizing on innovative ways to organize work that technology provides; the relationship 'gap' between the IS function and rest of the business (Peppard and Ward, 2009).

Ndulu (2011) in a survey of the causes of IS failure among Micro Finance Institutions (MFI) in Kenya identifies lack of adequate IT training among staff and lack of a formally documented IT strategy to which the IS implementation is aligned as some of the factors that influence IS failure. MFI also tend to suffer from an emphasis on technology rather than its information value. This results in unnecessary investments in IT which does not complement the business needs. Further, Ndulu observes that most MFI in Kenya lack adequate resources make supplementary investments necessitated by rapid technological changes rendering current systems obsolete.

Organisational stakeholders are important in determining what constitutes success or failure, and as such these models view IS development as socio-technical in nature. The socio-technical viewpoint in IS failure recognizes that problematic situations exist within the organisational context. Interaction failure then becomes a result of poor user attitude towards the IS in the various financial institution functions. This may occur due to resistance to change, IS illiteracy or poor information analytical skills. Change must also be dealt with from an application perspective. Pitman (2011) indicated that successful change depends on five critical factors, including visible management support and commitment, preparation for change, encouraging participation, supporting rewards and effective communication.

In support of this, Krovi (2009) contends that, in addition to technical proficiency, the success of strategic IS largely depends on how well firms implement such systems. Introducing any form of IS changes an organization to some extent, whether in its business, processes, culture or mission. Numerous businesses may fail in implementing IS owing to ignorance of organizational change. To reduce resistance to change, the IS implementation process should not only encompasses both business strategy and management control, but also consider change management.

Implicit support for the notion of a failure system can be found in Turner (2011) who argues that pre-failure signals accumulate until a crisis turns them into a failure. The factors responsible for failure are significantly social, administrative and managerial, rather than technical. Preconditions for failure, he terms as "pathogens" involve a multiplicity of minor causes, misinterpretations and miscommunications that are not resolved until they emerge as failure. In the case of the ICT in the marketing function, such minor causes may include an IS that fails to consider contextual variables such as organizational culture. Such IS provide information that is applicable in other social contexts, making it hard for managers to formulate relevant decisions.

User interaction may also be influenced by ergonomic factors. Ergonomics is the science of redesigning the workplace to meet the safety and health needs of the worker in order to prevent ailments such as Repetitive Strain Injuries (RSI), which are of say, the wrists and fingers. Ergonomics takes a holistic approach to the relationship between the work environment and human factors. It aims to improve job design to minimize monotonous and repetitive tasks, which may contribute to fatigue and stress. Wachira's (2007) study on ergonomic factors to consider in IS application revealed that users may be concerned about eye safety ("monitor glare") and RSI caused by repeated use of hardware tools (e.g. mouse). To encourage user interaction, such factors need to be considered by implementing tools such as anti-glare visors and system time-outs.

IS in financial institutions may also be prone to attacks by hackers, cyber criminals and insiders who seek to steal from or damage an organization. Individuals planning an attack have a wide array of attack options. Erasing customer data bases, planting virulent viruses or rifling through strategy correspondence are just a few of the attacks that may be directed at the victim's IS system. The use of IS has become more widespread and today's financial institution rely on IS to the extent that it would be impossible to manage without them. The growth of e-business and e-commerce applications also presents abundant opportunities for unauthorized access to IS (Brooks et al., 2005).

1.3. Online financial institution Risks

Financial institutions are subject to many online risk exposures. Wire transfer networks such as the international SWIFT inter financial institution fund transfer system are tempting as targets, since once a transfer is made, it is difficult or impossible to reverse. As these networks are used by financial institutions to settle accounts with each other, rapid or overnight wire transfer of large amounts of money are commonplace; while financial institutions have put checks and balances in place, there is the risk that insiders may attempt to use fraudulent or forged documents which claim to request a financial institution depositor's money be wired to another financial institution, often an offshore account in some distant foreign country.

There is a very high risk of fraud when dealing with unknown or uninsured institutions. The risk is greatest when dealing with offshore or Internet financial institutions (as this allows selection of countries with lax financial institution regulations), but not by any means limited to these institutions. Phishing, another form of online fraud, operates by sending forged e-mail, impersonating an online financial institution, auction or payment site; the e-mail directs the user to a forged web site which is designed to look like the login to the legitimate site but which claims that the user must update personal info. The information thus stolen is then used in other frauds, such as theft of identity or online auction fraud. A number of malicious “Trojan horse” programs have also been used to snoop on Internet users while online, capturing keystrokes or confidential data in order to send it to outside sites.

Although IS provides a powerful vehicle for processing information, the focus on technology has often shifted the emphasis away from the real issue of exploiting information for value creation to the delivery of technology. In general, IS has no inherent value in itself; for example, just having desktops on employees’ desks does not confer any value to the organization. This value must be unlocked and it is only business managers and users who can ensure that this occurs (Peppard et al., 2007).

In short, the ‘T’ of IT has become the focus of attention rather than the ‘I’. Yet the irony is that information is a factor of production while technology is a cost of doing business. Financial institution must redress the balance in favour of the ‘I’ if value is to be created (Peppard et al., 2007).

Meeting these opportunities and challenges requires technology infrastructures directed toward flexibility, openness and interconnectivity. It simultaneously entails a degree of local autonomy and control on localized service provision, as well as the ability to connect to external parties as needed. On the other hand, existing legacy, technical and organizational infrastructures for financial institutions are overwhelmingly closed, monolithic and inward directed. The legacy architectures make it difficult for these financial institutions to modify, develop and integrate their existing applications to meet the opportunities and challenges arising from deregulation, globalization and the changing demands of the market (Kumar and van Hillegersberg, 2011).

Recognizing the importance to generate value from IS, financial institution often engage in an examination of their IS function and many have looked towards the re-engineering of IS processes (Brown and Magill, 2009). However, such re-engineering effort generally only addresses the supply of technology into the business: the IS function becomes better at building and operating applications. Yet, these applications may only be contributing marginally to the achievement of organizational goals and objectives as the focus is on building and operating applications and technology rather than delivering significant business benefit (Peppard et al., 2007).

Developing measures of effectiveness has long been a focus of Management Information System research (Delone and McLean, 2011). Such techniques as system usage, cost/benefit analysis, information economics and critical success factors, have all been used with mixed results to gauge the contribution that information systems and the information services function make to firms and individuals. These same concerns are witnessed in the adaptation process, whereby MIS are used in enhancing given functions.

Also, implementing database and software systems for customer information management can be costly, difficult and time-consuming. Research is needed to understand whether and how, managing ICT in, say, the marketing function, in a particular strategic marketing context provides a sustainable competitive advantage. Again, there is the question of whether the organizational IS learning curve will lead to sustainable competitive advantage (Hult et al., 2007).

The efficacy of ICT in the marketing function is also determined by structural and cultural organizational capabilities. Structural capabilities include having a team and systems orientation, while cultural aspects of the organization’s ability to learn derive from how open the culture is and various qualities of its leadership (Deshpande, Farley and Webster, 2009). Cultural and structural capabilities undoubtedly influence an organization's ability to manage financial information systems.

A recent revolution, mobile financial institution is the provision of financial institution services through mobile phones using the SMS facility or a downloadable mobile money application. This collaboration between the financial and telecom sector is an ideal solution for microfinance (Toigo, 2009). Mobile financial institution (also known as M-Financial institution, SMS Financial institution, branchless financial institution) is quickly gaining momentum in

- Kenya (mobile financial institution through Safaricom’s M-Pesa – read the reasons behind its success and how it impacts the daily lives of Kenyans)

- Brazil (mobile financial institution through Banco de Brasil)
- India (mobile financial institution through FINO's MITRA:
- Pakistan (mobile financial institution through Telenor's Easy Paisa)
- Philippines (mobile financial institution through Smart Telecom's SmartMoney),and
- South Africa (mobile financial institution through South African Financial institution of Athens' Wizzit).

The following basic microfinance services are offered to meet every day needs of micro entrepreneurs and other clients:

- Cash deposits and withdrawal, through microfinance financial institution branches and other agents
- Micro loans provision and collection through mobile phones (clients are starting to give their feedback through surveys as well)
- Payment services for utility or other bills through mobile phones
- Money transfers between accounts, specifically remittances through mobile technology

Convenience, savings on transport costs, and security are the biggest advantages marketed to consumers by mobile financial institution, while MFIs get the benefit of reduced transaction costs and improved rural market penetration rates, which are difficult to access as it is.

2 Risk Mitigation

Information Risk Mitigation is the collection of processes that together ensures information risks are adequately reduced to a tolerable level. It includes the methods for identifying and assessing risks plus the methods for determining which controls need to be applied, for checking that those controls have been applied, and then for tracking the actual level of protection being achieved. Information Risk Mitigation is the collection of processes that together ensures information risks are adequately reduced to a tolerable level. It includes the methods for identifying and assessing risks plus the methods for determining which controls need to be applied, for checking that those controls have been applied, and then for tracking the actual level of protection being achieved.

Mitigation involves fixing the flaw or providing some type of compensatory control to reduce the likelihood or impact associated with the flaw. Sometimes the process of determining mitigation strategies is called control analysis. (Elky,2011)

Risk mitigation, according to the NIST Special Publication 800-30, involves prioritizing, evaluating, and implementing the appropriate risk-reducing controls recommended from the risk assessment process. Because the elimination of all risk is usually impractical or close to impossible, it is the responsibility of senior management and functional and business managers to use the least-cost approach and implement the most appropriate controls to decrease mission risk to an acceptable level, with minimal adverse impact on the organization's resources and mission. NIST (2002).

Risks should be assessed in terms of the general level of harm which could reasonably be caused if information systems were to fail or be compromised. Mitigation should take the form of a wide range of overlapping controls, some of which work to reduce the likelihood of an information failure and some of which work to reduce the amount of harm a failure can cause. A range of controls covering both aspects helps to ensure that, whatever the form in which a threat materializes, there is a good chance one or more controls will be in place to mitigate the risk.

Applying Good Practices across the organization provides a pragmatic approach to risk mitigation that everyone within the organization can understand and apply. Good Practice control baselines need to be supplemented by customized controls applied in specific higher-risk circumstances.

2.1 Risk Mitigation Options

Risk mitigation entails a methodical approach for evaluating, prioritizing and implementing appropriate risk-reduction controls, which includes security measures. A combination of technical, procedural, operational and functional controls would provide a rigorous mode of reducing risks.

Risk mitigation can be achieved through any of the following risk mitigation options ;the goals and mission of an organization should be considered in selecting any of these risk mitigation options.

- Risk Assumption -To accept the potential risk and continue operating the IT system or to implement controls to lower the risk to an acceptable level
- Risk Avoidance -To avoid the risk by eliminating the risk cause and/or consequence (e.g., forgo certain functions of the system or shut down the system when risks are identified)
- Risk Limitation -To limit the risk by implementing controls that minimize the adverse impact of a threat's exercising vulnerability (e.g., use of supporting, preventive, detective controls)
- Risk Planning -To manage risk by developing a risk mitigation plan that prioritizes, implements, and maintains controls
- Research and Acknowledgment -To lower the risk of loss by acknowledging the vulnerability or flaw

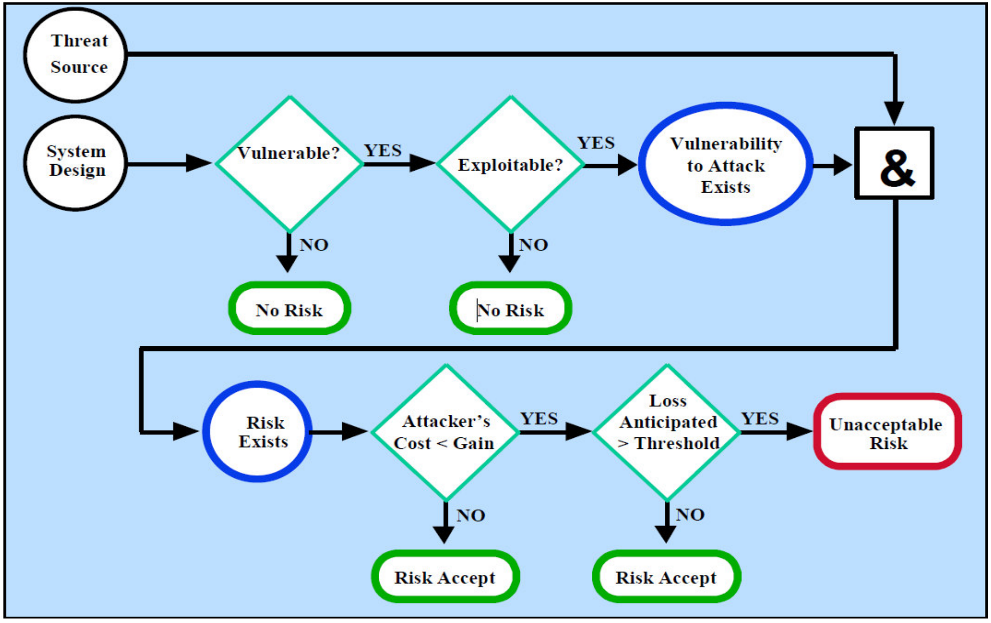
and researching controls to correct the vulnerability

- Risk Transference -To transfer the risk by using other options to compensate for the loss, such as purchasing insurance.

It may not be practical to address all identified risks, so priority should be given to the threat and vulnerability pairs that have the potential to cause significant mission impact or harm. Also, in safeguarding an organization's mission and its IT systems, because of each organization's unique environment and objectives, the option used to mitigate the risk and the methods used to implement controls may vary.

2.2 Risk Mitigation Strategy

The risk mitigation chart below indicates; when and under what circumstances should action betaken, when to implement controls to mitigate the risk and protect the organizations' systems.



2.3 Risk Mitigation Methodologies and Standards

Methodologies and standards should be consistent throughout the organization to provide confidence that risk mitigation efforts expended in one place are not being undermined by weaknesses allowed elsewhere. Consistent methodologies help to ensure consistent practice across the organization and enhance interoperability and versatility. An organization can take guidance from recognized external standards but must expect to develop its own standards according to its own particular needs.

Other main national and international standards relevant to Information Risk Mitigation include:

- ISO 9000 series – the ISO standard for quality management systems
- ISO 27000 series (formerly BS 7799 and ISO
17799) – best practice recommendations for information security management systems
- BSI DISC PD0008 – the British standard relating to the legal admissibility and evidential weight of information stored electronically
- BS 25999 – the British standard for Business Continuity Planning
- BS 25777 (formerly PAS 77) – a code of practice for IT Service Continuity Management
- COBIT – internationally recognized guidance for IT Governance and Control

3 Monitoring and Review

No matter how diligently an organization strives to ensure it has all appropriate controls in place, protection failures will arise from time to time. Organizations need to monitor for protection failures so they can deal with incidents as they arise and contain the harm those incidents cause. Organizations also need to keep the number and nature of their incidents under review so they can learn the available lessons. Incidents provide a rare objective indicator of the real level of risk being experienced, and should be used to benchmark and adjust the risk mitigation controls in place.

The organization's objectives, its internal structures and systems, and the environment in which it operates, are continually evolving. As a result, the risks the organization faces are continually changing. A sound system of information risk mitigation will include the regular re-evaluation of the nature and extent of the risks to which the organization is exposed, plus periodic adjustment to ensure the organization continues to steer the line between allowing risks to grow out of hand and constraining operational effectiveness.

The assumptions made in the previous risk assessment (hazards, likelihood and consequence),the effectiveness of controls and the associated management system as well as people need to be monitored on an on-going basis to ensure risk are in fact controlled to the underlying criteria. For an efficient risk control the analysis of risk interactions is necessary. (Berg, 2010)

The organization should maintain a risk register which facilitates the monitoring and reporting of risks. Risks of the highest severity should be accorded top priority and monitored closely with regular reporting on the actions that have been taken to mitigate them. The information system risk management team should update the risk register periodically, and institute a monitoring and review process for continuous assessment and treatment of risks. (MAS, 2013). Risks of the highest severity should be accorded top priority and monitored closely with regular reporting on the actions that have been taken to mitigate them. A monitoring and review process should also be instituted for continuous assessment and treatment of risks.

It is important to understand that the concept of risk is dynamic and needs periodic and formal review. New risks and their impact on the organization may to be taken into account. This step requires the description of how the outcomes of the treatment will be measured .Milestones or benchmarks for success and warning signs for failure need to be identified. The review period is determined by the operating environment (including legislation).

In view of changes in IT environment and delivery channels, risk parameters may change. Thus, the risk processes should be reviewed and enhanced accordingly. Re-evaluation of past risk-control methods with renewed testing and assessment of the adequacy and effectiveness of risk management processes should be conducted. Management should review and update its risk control and mitigation approach, taking into account changing circumstances and variations in its risk profile.(MAS, 2013)

3.1 Communication, Consultation and reporting

Consultation and communication is both a key component of the risk management process and highly beneficial. Successful risk management relies on achieving a high level of creative input and involving all parties with a role to play in achieving a successful outcome for the project or business process being addressed. In both the planning and execution of the risk management process, it is important to ensure that all those who need to be involved are given adequate opportunity to do so and are kept informed of developments in the understanding of risks and the measures taken to deal with them. (AS/NZS 2009)

The operation of the risk management process offers many opportunities for cost-effective communication between people working on a project or business. The context statement is a concise summary of the most important features of the task; its objectives and scope, who is involved, how success will be assessed and how it can be broken into parts for analysis. Participation in a risk workshop offers opportunities for focused communication and naturally directs attention towards the highest priority issues. A risk register based on the workshop output and subsequent treatment planning provides a concise summary of the major uncertainties being addressed and once again ensures a focus on high priority issues.(AS/NZS 2009)

Clear communication is essential for the risk management process, i.e. clear communication of the objectives, the risk management process and its elements, as well as the findings and required actions as a result of the output. Risk management is an integral element of organization´s management. However, for its successful adoption it is important that in its initial stages, the reporting on risk management is visible through the framework. The requirements on the reporting have to be fixed in a qualified and documented procedure, e. g., in a management handbook.

Documentation is essential to demonstrate that the process has been systematic, the methods and scope identified, the process conducted correctly and that it is fully auditable. Documentation provides a rational basis for management consideration, approval and implementation including an appropriate management system. This document is a basis for communication throughout the organization and for the on-going monitor and review processes. It can also be used with other supporting documents to demonstrate regulatory compliance. (Gustavsson, 2011, Berg, 2010)

Once risk is understood, risks and risk management strategies must be clearly communicated to organizational management in terms easily understandable to organizational management. Managers are used to managing risk, they do it every day. So presenting risk in a way that they will understand is key .present risk in terms of likelihood and impact. The more concrete the terms are, the more likely organizational management will understand and accept the findings and recommendations.

With a quantitative risk assessment methodology, risk management decisions are typically based on comparing the costs of the risk against the costs of risk management strategy. A return on investment (ROI) analysis is a powerful tool to include in the risk assessment report. This is a tool commonly used in business to justify taking or not taking a certain action. (Elky, 2011)

With a qualitative risk assessment methodology, the task is somewhat more difficult. While the cost of the strategies is usually well known, the cost of not implementing the strategies is not, which is why a qualitative and not a quantitative risk assessment was performed. Including a management-friendly description of the impact and likelihood with each risk and risk management strategy is extremely effective. Another effective strategic is showing the residual risk that would be effective after the risk management strategy was enacted.

(Elky, 2011)

4. Conclusion

It is very important for any financial institution to decide on the risk mitigation and monitoring strategies and options that will suit their unique situations in order to minimize the losses that would be incurred. To facilitate risk reporting to management, information system risk metrics should be developed to highlight systems, processes or infrastructures that have the highest risk exposure. An overall information system risk profile of the organization should also be provided to the board and senior management. In addition, risk events, regulatory requirements and audit observations should be considered in determining the information system risk metrics. (MAS, 2013).

References

AS/NZS 4360:2009, Tutorial: Risk Management Standard, Broadleaf Capital International, Broadleaf Capital International Pty Ltd

Bell, J. (2008), *Doing Your Research Project*, London: Open University.

Bella, D. (2011), Financial institution and Systematic Distortion of Information, *Journal of Professional Issues in Engineering*, 113(4), pp. 360-70

Berg H., 2010; Risk Management: Procedures, Methods And Experiences. Vol.1).BundesamtfürStrahlenschutz, Salzgitter, Germany

Blumenstein, H. J (2007), The Changing Nature of Risk and the Challenges to Sound Risk Management in the New Global Financial Landscape, *Financial Market Trends*, pp 174 – 194

Brooks, W. J., Warren, M. J. and Hutchinson, W. (2011), A Security Evaluation Criteria, *Logistics Information Management*, 15(5/6), pp. 377-84.

Cadle, J. and Yeate, D. (2007), *Project Management for Information Systems*, Financial Times/Prentice-Hall, Harlow.

Central Financial institution of Kenya [CBK] (2010), *The Commercial Financial institution Sector in Kenya* [Online], Available from: www.cbk.go.ke [Cited 22nd April 2010]

Commonwealth of Australia (1996) Guidelines for Managing Risk in the Australian Public Service. MAB/MIAC Report 22, AGPS, Canberra.Deery, H. (2008), Hazards and Risk Perception among Young Novice Drivers, *Journal Of Safety Research*, 30(4), pp. 225-36.

Cooper, DF, SJ Grey, GA Raymond and PR Walker, Project Risk Management Guidelines:
Managing Risk in Large Projects and Complex Procurements, John Wiley & Sons, Chichester,
2009. ISBN 0 470 02281 7.

Delone, W. H. and Mclean, E. R. (2010), Information Systems Success: The Quest for the Dependent Variable, *Information Systems Research*, 3(1), pp. 60-95.

Deshpande, R., Farley, J. U. and Webster, F. E., Jr. (2008), Corporate Culture, Customer Orientation and Innovativeness in Japanese Firms: A Quadrad Analysis, *Journal Of Marketing*, 57(January), pp. 23– 37.

Douglas, M. (2010), *Risk and Blame: Essays in Cultural Theory*, Routledge, London.

Douglas, M., Wildavsky, A. (2011), *Risk and Culture: An Assay on the Selection of Technological and Environmental Dangers*, University of California Press, Berkeley, CA.

Dowd, K. (2008), *Beyond Value at Risk*, John Wiley and Sons, NY.

Drucker, P. (2011), *Management: Tasks, Responsibilities*, Practices, W. Heinemann, Ltd, London.

Edwards, B. (2010), Developing a successful disaster recovery plan, *Information Management and Computer Security*, 2(3).

Elky S., (2011).An Introduction to Information System RiskManagement.SANS Institute

Fitzgerald, K.J. (2010), The importance of a network disaster recovery plan, *Information Management and Computer Security*, 2(1).

Frosdick, S. (2011), The Techniques of Risk Analysis are Insufficient in Themselves, *Disaster Prevention and Management*, 6(3), pp.165-77.

Gerber, M., Von Solms, R. (2011), Management of Risk in the Information Age, *Computers and Security*, 24(1), pp.16-30.

Goulielmos, M. (2009), Outlining Organizational Failure in Information Systems Development, *Disaster Prevention and Management*, 12(4), pp. 319-327

Hansche, S. (2007), Designing a Security Awareness Program: Part I, *Information Systems Security*, 9(6), pp.14-22.

Heng, G. M. (2008), Developing a Suitable Business Continuity Planning Methodology, *Information Management and Computer Security*, 4(2).

Hult, G. T. M., Ketchen, D. J., Jr. and Slater, S. F. (2011), A Longitudinal Study of the Learning Climate and Cycle Time in the Supply Chain, *Journal of Business and Industrial Marketing*, 17(4), pp. 302– 322.

Institute Of Risk Management (2011), *A Risk Management Standard*, Airmic, Alarm, Irm, available At: www.theirm.org/ (accessed 4 October 2011).

Karakasidis, K. (2011), A Project Planning Process for Business Continuity, *Information Management and Computer Security*, 5(2).

Karyda, M., Kiountouzis, E. and Kokolakis, S. (2011), Information systems security: a contextual perspective, *Computers and Security Journal*, 24(3), pp. 246-60.

Kasperson, R. (2010), "The Social Amplification of Risk: Progress in Developing an Integrative Framework", In Krimsky, S., Golding, D. (Eds), *Social Theories of Risk*, Praeger, London, 6, pp. 153-78.

Kumar, K. and van Hillegersberg, J (2010), New architectures for financial services: Introduction, *Communications of the ACM*, 47(5), pp. 26-30

Lyytinen, K. and Hirschheim, R. A. (2011), Information Systems Failures: A Survey and Classification of the Empirical Literature, *Oxford Surveys in Information Technology*, 4, pp. 257-309.

Monetary Authority Of Singapore(Mas) (2013), Technology Risk Management Guidelines;Consultation Paper,P012 – 2012

National Institute of Standards and Technology Special Publication 800-30, Risk Management Guide for Information Technology Systems (July 2002)

NIST (2002); NIST Special Publication 800-30; Risk Management Guide for Information Technology Systems.National Institute of Standards and Technology. 1Booz Allen Hamilton Inc. 3190 Fairview Park Drive Falls Church, VA 22042

Nunes, M. and Annansingh, F. (2011), "The risk factor", *The Journal of the Institute for the Management of Information Systems*, 12(6), pp.10-12.

Peppard, J. W. and Ward, J. M. (2008), Mind the gap: diagnosing the relationship between the ICT organisation and the rest of the business, *Journal of Strategic Information Systems*, 8, pp. 29–60

Peppard, J., Lambert, R. and Edwards, C. (2007), Whose job is it anyway? Organizational information competencies for value creation, *Information Systems Journal*, 10(4) p. 291

Sauer, C. (2008), *Why Information Systems Fail: A Case Study Approach*, Alfred Waller, Henley on Thames.

Simon, J.C. (2007), *Introduction to Information Systems*, John Wiley & Sons, New York, Ny.

Siponen, M. (2007), A Conceptual Foundation for Organizational Information Security Awareness, *Information Management & Computer Security*, 8(1), pp. 31-41.

Sjoberg, L. (2007), Factors In Risk Perception, *Risk Analysis*, 20(1).

Slovic, P., Fischoff, B., Lichtenstein, S. (2009), "Facts and Fears: Understanding Perceived Risk", In Schwing, R. C. and Albers, W. A. (Eds), *Societal Risk Assessment:. How Safe Is Safe Enough?* Plenum, London, pp. 181-216.

Smallman, C. and Weir, D. (2008), Communication and Cultural Distortion during Crises, *Disaster Prevention and Mangement*, 8(1), pp. 33-41

Soliman, K. S. and Janz, B. D. (2010), An Exploratory Study to Identify the Critical Factors Affecting the Decision to Establish Internet-Based Interorganizational Information Systems, *Information & Management*, 41(3), pp. 697-706.

Stair, R. M. and Reynolds, G. W. (2008), *Principles of Information Systems*, Course Technology (ITP), London

Standards Australia and Standards New Zealand (2009) HB 436:2009, Risk Management
Guidelines: Companion to AS/NZS 4360:2009, Sydney, NSW. ISBN 0 7337 5960 2.

Toigo, J. (2008), *Disaster Recovery Planning for Computers and Communication Resources*, John Wiley, & Sons, New York, NY.

Torbjorn, R. (2010), *Explaining Risk Perception: An Evaluation of Cultural Theory*, Norwegian University of Science and Technology, Norwegian University of Science and Technology, Department Of Psychology, Trondheim, 85.

Turner, B.A. (2010), Causes of Disaster: Sloppy Management, *British Journal of Management*, 5, pp. 215-19.

Van Teijlingen, E. R. and Hundley, V. (2007), *The Importance Of Pilot Studies* [Online], Social Research Update, Issue, 35, Department of Sociology, University of Surrey, Guildford Gu7 5xh, England, Available From: http://www.soc.surrey.ac.uk [cited 22nd April 2010] publication available from website

Varcoe, B. J. (2010), Not Us, Surely? Disaster Recovery Planning for Premises, *Facilities*, 12(9)

Wachira, A. (2007), *Ergonomic Factors Considered in Information Systems Implemented in Kenya. The Case of Firms in Nairobi*, published MBA Research Project, University of Nairobi, Nairobi, Kenya

Whitman, M., Towsend, A. and Aalberts, R. (2007), "Information systems security and the need for policy", in Dhillon, G. (Eds), *Information Security Management: Global Challenges in the New Millennium*, Idea Group Publishing, Harshey, PA.