Journal of Information Engineering and Applications
ISSN 2224-5782 (print) ISSN 2225-0506 (online)
Vol.4, No.3, 2014
www.iiste.org

# Risk Management in Financial Information Systems using Bayesian Networks

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**
During the last 20 years many technological advances have inundated the entire spectrum of our everyday lives. None of these advances has had such an impact like the IT revolution which can only compare with the Industrial Revolution of the 18th Century. The advent and acceptance of Information Technology as the norm rather the exception has seen this sector move from a tedious and cumbersome manually managed and run sector, to an almost paperless industry that is almost entirely dependent on Information Systems. With the growth of the dependency on IT, the impact of risk concerns on the development and exploitation of information systems has also increased exponentially. Within the financial services industry, risk management involves assessing and quantifying business risks, then taking measures to control or reduce them. These methods are generally built around a well structured process. However, the product coming from the different risk management steps is still largely informal, and often not analytical enough. This lack of formality hinders the automation of the management of risk-related information. Furthermore, these risk management system focuses on specific phases of the software life cycle, without recognizing that risks in one stage can have an impact on other stages. This necessitates the proposed study in order to propose a generic approach that may be deployed to mitigate risks from the early stages of financial information systems development for daily financial institution operations until the post-implementation phases. This paper proposes a new approach for performing a risk analysis study of financial information systems. It is aimed at developing a generic approach for Risk Analysis and Management applicable from the early phases of information system development unlike in the existing models which are applied after the development process. It can be utilized for identifying and valuating the assets, threats, and vulnerabilities of the information system, followed by a graphical modeling of their interrelationships using Bayesian Networks. The proposed approach will exploit the results of the risk analysis for developing a Bayesian Network model, which presents concisely all the interactions of the undesirable events for the system. Based on "what–if" studies of system operation, the Bayesian Network model identifies and prioritizes the most critical events.
**Keywords:** Riks, risk management, Bayesian Network model

## *1. Introduction*

Information Communication Technology (ICT) has become an attractive means of improving the process of gathering information (Soliman and Janz, 2010). 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, 2011), while The Computer Security Institute (CSI) (2011) 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., 2010).

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, 2011). 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.

### *1.1 Nature of Risk and Risk Management*

Douglas and Wildavsky (2011) indicates that one of the oldest and most accepted generalizations in decision theory is that people are generally risk averse. They are also assumed to prefer certainty to uncertainty. However, in practice and against established theory, people are not risk averse for negative prospects, only for positive ones; so we actually are creatures who habitually tolerate risk. Conventional risk analysis assumes that individuals are free to express their will and that there is no such thing as society.

This thinking is misleading and potentially harmful. 'In risk perception, humans act less as individuals and more as social beings who have internalized social pressures and delegate their decision-making processes to institutions. They manage as well as they do, without knowing the risks they face, by following social rules on what to ignore: institutions are their problem simplifying devices.'

Thus, to assume individual preferences as being rational and consistent also ignores the degree of socialization of individual attitudes to risk and the role institutions play in managing or simplifying these risks. The individual preferences cannot be divorced from ethical beliefs and value judgments, and if risk is to be properly understood, the experts need to go beyond the boundaries of their disciplines (Shah, 2010).

In most cases, the probabilities for risk analysis are uncertain, the set of possible outcomes is unclear, and our perception of both is affected by a host of subjective factors i.e. the perception of risk is a complex and subjective process. The fear factor and control factor (the extent to which we are in control of events) are two major components of risk that influence our perceptions.

In making risky decisions, two factors are significant (Pickford, 2007). One major component of risk perception is how we perceive loss and gain. Some individual may emphasize the importance of reputation as well as gain. Our perceptions of our current state of loss or gain influence the extent to which we seek or avoid risk. Emanating from the present theory is a principle that people tend to make different choices under different conditions. When people are in a position of gain, they become increasingly risk averse and unwilling to accept gambles because they wish to hold on to their gains.

When people are in a position of loss and as losses increase, they become more risk seeking since they have nothing much to lose. This asymmetry also applies to losses and gains. However, what we perceive as loss and gain is not straightforward. We all have internal reference points that determine whether we perceive an outcome as a loss or gain. These reference points also shift over time. The effects of loss and gain can also operate at the group or team level.

Decision making about risk often departs from the prescriptively rational model. Cognitive biases influence much of our everyday thinking (Pickford 2007). These biases often arise out of heuristics that act as short cuts to enable us to process information quickly or simplify complex situations. They act as rules of thumb. One's own innate disposition can create preferences that underline characteristic ways of perceiving the risk in ones environment and whether the situation is seen as an opportunity or threat.

Therefore, both personal and organizational factors can shape ones perceptions about risk. Illusion of control is a cognitive bias that involves holding beliefs concerning the extent to which we are able to exert control over events in which we are involved and over tasks we undertake. Many of these beliefs arise out of experience. Research has shown that illusion of control may lead to poor risk management. Managers need to be aware of conditions that encourage this bias.

Beck (2010) contends further that many of the risks taken by modern society are unknown. The process of risk evaluation on people can only be studied reliably with people. Society is therefore becoming a laboratory. Beck was particularly critical of the isolation of ordinary people from risk evaluation and the influence of scientists in calculation of acceptable levels. Thus, we should be very skeptical of accepting science-based solutions to the problem of risk. Asaf (2010) also notes that business risk management combines a little of science with a great deal of subjective judgment.

Risk management is not unique to the IT environment; indeed it pervades decision-making in all areas of our daily lives. Take the case of home security, for example. Many people decide to have home security systems installed and pay a monthly fee to a service provider to have these systems monitored for the better protection of their property. Presumably, the homeowners have weighed the cost of system installation and monitoring against the value of their household goods and their family's safety, a fundamental "mission" need.

Business risk comes in many forms. Asaf (2010) indicates that the types of risks companies are exposed to, can be divided into five main groups:

Strategic risks include risks of plans failing, poor corporate strategies, or even adverse political or regulatory change. Political risk refers to the threat posed by new regulations and expropriation. Financial risks include risks of financial controls failing, treasury risks, lack of counterparty credit assessment, sophisticated financial fraud and the effect of changes in macroeconomic factors. Interest rate risk and foreign currency risk are the main categories of financial risks.

Operational risks arise from business operations, including risks of human error or omission, design mistakes, unsafe behavior, employee practice risks and sabotage; Commercial risks on the other hand, include risks of

business interruption, loss of a key executive, supplier failure and lack of legal compliance; while technical risks encompass risks of physical assets failing or being damaged, equipment breakdown, infrastructure failure, fire, explosion and pollution

Operational risk management is therefore aimed at helping financial institution identify and mitigate potentially adverse events ahead of time. Operational risks are unique to each business based on: industry, competitive structure, customer demographics, demand and supply conditions, sensitivity to economic conditions, product elasticity's to various factors, level of complexity in product development and delivery and intangible issues such as intellectual rights and level of human capital intensity (Blumesntein, 2007).

Operational risk management is a relatively new management discipline with the goal of enhancing management performance through the early identification and avoidance of business disruption. Its specific focus is on failure of people, processes, systems or external events. By its nature, operational risk management is the integration of risk management with core operations management. In the 1990 and 2009, much of the focus on corporate risk management revolved around designing and implementing control frameworks, managing insurance portfolios and meeting corporate governance standards. In the dawn of the twenty-first century, leading companies are rethinking the nature of risk, risk management and operations management (Copeland et. al. 2010).

Operational risks also include the risk that failure in computer systems, internal supervision and control and natural events will impose unexpected losses on a firm's performance. Other operating risks may include excessive operating leverage and legal risks (Dowd, 2008). Risks should be categorized in accordance with the goals of the organization. The following questions must be asked of the organization in order to determine priorities and goals:

a. What is the organizational and legal status of this agency? (For example, profit, non-profit, public, private and cooperative).
b. Who is the organization accountable to?
c. What is the scope and value of the organization's assets?
d. Which digital assets does this organization need to preserve?

This generalized risk process begins with human or natural activities which give rise to loadings or accident initiating events. These, in turn, lead to exposures and effects, which are then perceived and valued by people. Within each stage of the process, categories of risk can be established and risks within these can then be ranked (Douglas and Wildavsky, 2011).

### *1.2 The Risk Management Process*

According to the Institute of Risk Management (2011), there is a variety of views and descriptions of the processes that risk management involves, the way it should be conducted and what is aimed at. Three stages to consider in assessing and managing risk include (Crabb, 2009):

a. Risk identification or initiation incorporates issues on resources at risk, type of threats, value of resources and organizational vulnerabilities. Identifying risk scenarios should begin with an understanding of how the system should work.
b. Risk analysis deals with levels of acceptable risk, likelihood of risk materializing, direct and indirect costs, consequences of risk materializing and safeguards in place, and
c. Risk mitigation which focuses on mitigation options and responses, risk prioritization, management strategies, risk reduction and tradeoffs.

## 2 Risks Underlying New Systems Development

The risk of computer systems failing requires financial institution to put in place countermeasures to combat the effects of an interruption to business. The Computer Services Association defines a business disaster as any accidental, natural or man-made malicious event which threatens to or does disrupt normal operation or service for a sufficient time to affect significantly, or to cause failure of, the organization. Other writers view a disaster as being the failure to access mission critical information for significant periods (Toigo, 2008). In many instances business disasters may be personal to every individual organization. However, business continuity plans should concentrate on mission-critical or core systems (Fitzgerald, 2010) where failure equates directly to lost business.

Many companies do not have business continuity plans in place even though the relevance and importance of risk management procedures may never have been more significant (Renkema, 2007). The purpose of these plans should be to ensure the business survives rather than just the recovery of their computer systems (Edwards, 2010). Financial institution should be able to absorb the effect of a system disruption on its business. Varcoe (2010) viewed risk planning as carrying out a risk assessment; undertaking a business impact assessment; and preparing a business continuity plan. Heng (2008) viewed the approach as, performing an impact analysis; determining processing requirements; and, finally, risk analysis. Karakasidis (2011) gives more detail as indicated below about raising awareness of the business recovery process:

a. Define the objectives, scope and success factors of the business continuity process;

b. Manage the development of all required business recovery procedures for core business activities;
c. Support business recovery testing and maintenance; and
d. Support a business recovery awareness program.

It appears that many financial institutions are taking a risk with the development of their information systems. In essence they are acting without regard to the business risks involved. Majority of writers in the area of information systems view risk as something to be addressed once the system is up and running, i.e. fire, fraud, computer failure and unauthorized access (Simon, 2007). This appears to align with the focus adopted by many current risk management methodologies.

The significant increase in the number of distributed systems environments, with nearly every employee having access to systems, has made the security issue more critical. Systems auditors may be interested in safeguarding assets, data integrity, system efficiency and effectiveness. It would be wrong to assume that just because a risk assessment can be undertaken that it can then be controlled (Laudon and Laudon, 2008).

However, there are many risk factors to consider before the information system goes live. Some writers believe that the information systems implementation process is as important for IS success as the information system itself (Kwon and Zmud, 2011). There are many things that can go wrong during the process of system development and financial institution should be simultaneously attempting to reduce risk and increase security during system implementation. The integrity of organizational information systems needs to be seen as a high priority.

The extra pressure placed on information systems resources has made this investment often large and risky. Many financial institutions have totally integrated systems that also link with customers and suppliers. The financial consequences of system failure make it necessary to develop a strong link between risk and cost-benefit analysis (Curtis and Cobham, 2011). This could be an important part of the strategic planning process. Risk could then be assessed under different headings such as:

a. Risks associated with new technology;
b. Risks associated with project size;
c. Risk of failure, i.e. the damage that can be done to the firm if the project fails.

If a project is ambitious i.e. a Business Process Re-engineering (BPR) project, the risk of failure may increase proportionately (Stair and Reynolds, 2008). The success of the system development may be dependent on the organization's ability to manage change. If the system can be copied quickly by competitors there may be financial risks in investing too heavily in a new project.

In a particular business sector it may be difficult to sustain even a short-term competitive advantage. It may be difficult to successfully implement and maintain profitable information systems. However, without systems innovation an organization could find itself at a strategic risk. Before investing in new information systems, management should assess the company's position in relation to:

a. Monetary resources;
b. Technological sophistication; and
c. Organizational flexibility.

***2.1 Integration of Risk Management into SDLC***

Minimizing negative impact on an organization and need for sound basis in decision making are the fundamental reasons financial institution implement a risk management process for their Information systems (Delone and McLean, 2010). Effective risk management must be totally integrated into the SDLC. In some cases, an Information system may occupy several of these phases at the same time. However, the risk management methodology is the same regardless of the SDLC phase for which the assessment is being conducted. Risk management is an iterative process that can be performed during each major phase of the SDLC. The table below describes the characteristics of each SDLC phase and indicates how risk management can be performed in support of each phase.

Table 1: Integration of Risk Management into SDLC

| SDLC Phases | Phase Characteristics | Support from Risk Management Activities |
|---|---|---|
| Phase 1—Initiation | The need for an IT system is expressed and the purpose and scope of the IT system is documented | • Identified risks are used to support the development of the system requirements, including security requirements, and a security concept of operations (strategy) |
| Phase 2—Development Or Acquisition | The IT system is designed, purchased, programmed, developed, or otherwise constructed | • The risks identified during this phase can be used to support the security analyses of the IT system that may lead to architecture and design trade- offs during system development |
| Phase 3— Implementation | The system security features management process should be configured, enabled, the assessment of the tested, and verified implementation against | • The risk supports system its requirements and within its modeled operational environment. Decisions regarding risks identified must be made prior to system operation |
| Phase 4—Operation or Maintenance | The system performs its functions. Typically the system is being modified on an ongoing basis through the addition of hardware and software and by changes to organizational processes, policies, andprocedures | • Risk management activities are performed for periodic system reauthorization (or reaccreditation) or whenever major changes are made to an IT system in its operational, production environment (e.g.,new system interfaces) |
| Phase 5—Disposal | This phase may involve the management activities disposition of information, for system hardware, and software.components that will be Activities may include moving,replaced to archiving, discarding, or that the hardware and destroying information and properly disposed sanitizing the hardware and residual data is software appropriately handled, and that | Risk are performed disposed of or ensure software are of, that system migration is conductedin a secure and systematicmanner |

### *2.2 Risks Faced in Applying Information Systems in the Financial Institutions*

Despite cases of successful IS development projects, various estimates show persistently that half of all systems fail. 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 (2011) 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 (2008) 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, 2009).

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, 2008).

Ndulu (2010) 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 (2010) 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 (2008) 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 (2010) 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., 2011).

## 3 Application of Bayesian Networks

Bayesian network is a directed acyclic graph with vertices representing random variables and arcs define dependencies. The existence of an arc between two vertices means that there is a cause and effect the direct relationship between the corresponding variables (BayesianLab,2010). The concept of Bayesian Networks is based on conditional probability. Based on the observation of the real world can make a finding that there are many situations where the occurrence of one event depends on another event. Using Bayesian networks can avoid the computation of high complexity. The calculation of the one a 'posteriori probability is linked with another used probabilities (a concept of directed acyclic graph). Bayesian network is a numerical model of cause and effect relationship occurring between the elements of a set of observations and hypotheses. Using Bayer's theorem we can make inference progressive (forward inference) and regressive (backward reasoning), which Bayesian networks are often used in the

inference of partial and uncertain knowledge (G. Suchacka, Z. Zgrzywa, 2001). This uncertainty is often dependent on the following factors:

• Uncertainty as to the expert knowledge;
• Uncertainties inherent in the modeled area;
• Uncertainty resulted from the accuracy of their knowledge

Bayesian networks are based on probability theory; they are used to determine the uncertainty by explicitly representing the conditional dependencies between different parts of the knowledge. This makes possible an intuitive graphical visualization of knowledge in the form of graphs, including the interactions between the different sources of uncertainty (K. P. Murphy, 2002).

### *3.1 Bayes theorem*

Bayes theorem [Jakubowski 2008], is based directly on the conditional probability, where the probability of event $A$ is calculated in a situation where we have the certainty of an event $B$. If an event $B$ has no effect on the probability of event $A$, then events $A$ and $B$ are independent. If A is a primary event (cause), and B is a secondary event (effect) and assuming that $P(A) > 0$ and $P(B) > 0$, then using the definition of conditional probability we

obtain

$$P(A \cap B) = P(A)P(B \mid A) = P(B)P(A \mid B)$$

……(1)

where the conditional probability of occurrence of an event *A*, provided that the occurrence of event *B*, on the assumption that $P(B) > 0$, then the number

$$P(A \mid B) = \frac{P(A \cap B)}{P(B)}$$

……(2)

Using the assumptions contained in [2], if *Ai*, for $i = 1,2,..., n$, will mean mutually exclusive pairs of primary events whose sum is a certain event

$$\bigcup_{i=1}^{n} A_i = \Omega$$

……(3)

and *B* will mean a secondary event, where $P(B) > 0$, then using the theorem of total probability we obtain

$$P(B) = \sum_{i=1}^{n} P(A_i)P(B \mid A_i)$$

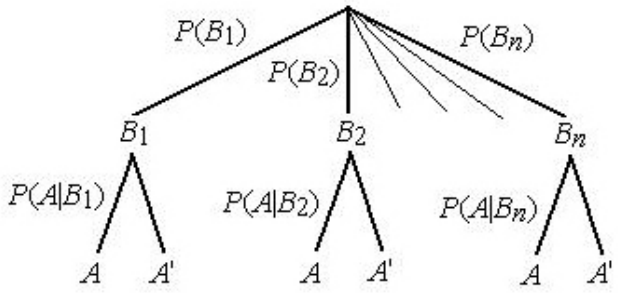
……(4)

The formula (4) follows directly from the argument using the formula (1)

$$P(B) = P\left(\bigcup_{i=1}^{n}(B \cap A_i)\right) = \sum_{i=1}^{n} P(B \cap A_i) = \sum_{i=1}^{n} P(A_i)P(B \mid A_i)$$

….. (5)

Total probability of occurrence of an event *B* can be represented in the form of so called. stochastic tree




***Stochastic tree***

Total probability of event B is the sum of products of all the conditional probabilities of the event *B*. Finally, the formulas (1) and (4) shows the Bayesian model

$$P(A_i \mid B) = \frac{P(A_i)P(B \mid A_i)}{\sum_{i=1}^{n} P(A_i)P(B \mid A_i)}$$

…… (6)

Information appearing on the right side of equation (6) is called *a'priori* information (apriori), which means that the observed occurrence of an event occurrence of *Ai* and analyzed the effects in the form of an event *B*, which is possible to determine the probabilities P(Ai) and *P(B| Ai)* on the basis of past experience. The probability *P(Ai|B)* is called the probability *a'posteriori* (after experience), which means the occurrence of an event *A* provided that the event *B* occurred.

### *3.2 Modelling Bayesian Networks for Risk Management*

Building a Bayesian network model for this problem, we should specify the network topology, thus the total probability distribution of the network variables is described by the

Equation (6):

$$P(X_1,\cdots,X_n)=\prod_{i=1}^{n}P(X_i \mid \prod(X_i)) \qquad \text{……..(7)}$$

Whereby, we denote the set of parents of a node in the graph.

***3.3 Bayesian network model for risk rating system for financial information system success***

Analyzing the problem discussed in the article, you can specify a set of conditions (hypotheses), which will form the basis for determining the likelihood of an incident of success or failure of financial information systems. Using the total probability theorem and Bayes' theorem, we can build a Bayesian network model based on the conditions set.

***3.4 Introduction to building a system to assess the risk of financial information system failure***

The Bayesian network model is the basis for further deliberations on the system giving the possibility of an effective risk assessment, which may occur when developing a financial information system. This model as shown in the diagram below will be a generalization of the most important conditions affecting the occurrence of events that directly or indirectly affect the success of business investment. The weights of the conditions are dependent on the type of financial information system and the institution where the project is carried out. Therefore extremely important aspect is the process of learning Bayesian networks, aimed at assessing the various parameters and updating the probabilities based on entered data. More research should be done on the proposed framework in order to refine it and use Bayesian inference so that the Bayesian network can readily be updated when more data becomes available.

## 4. Conclusion

It is evident that there are many risks facing information systems especially in the financial sector which is very sensitive. It is therefore important to note that these risks need to be assessed and managed in the best way possible right from the start of the system development process. Study risk of failure of financial information system is undoubtedly an important issue in the design and implementation of IT systems. Despite the great tools and advanced design methodologies still a huge number of financial information systems fail. Properly designed and learned Bayesian networks give the opportunity to determine whether a financial information system is a success or failure right from the initial development process unlike during the implementation process. Taking into account the enormous costs of the implementation of most systems, detect errors in various stages of development will achieve measurable gains.

## References

Asaf, S. (2010), *Executive Corporate Finance*, London, Prentice Hall

Baker, T. L. (2010), *Doing Social Research* (2nd Ed.), New York: Mcgraw-Hill Inc.

Baskerville, R. (2008), Risk Analysis: An Interpretive Feasibility Tool in Justifying Information Systems Security, *European Journal of Information Systems*, **1**(2), pp.121-30.

Beck, U. (2010), *Risk Society: Towards a New Modernity*, Sage Publications Inc.

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

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]

Copeland, T. and Weston, J. (2010), *Financial Theory and Corporate Policy*, Addison-Wesley

Curtis, G. and Cobham, D. (2011), *Business Information Systems: Analysis, Design and Practice*, Financial Times/Prentice-Hall, Hemel Hempstead.

Deery, H. (2008), Hazards and Risk Perception among Young Novice Drivers, *Journal Of Safety Research*, **30**(4), pp. 225-36.

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).
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).
J.V. Finn (1996), An Introduction to Bayesian Networks, UCL Press, Londan (1996).
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.
Kinyanjui, J. W. (2007), *A Survey of Work Values and the Use of Information Systems. A Case of Selected Business Firms in Kenya*, Unpublished MBA Research Project, University of Nairobi, Nairobi, Kenya
Kotler, P. and Armstrong, G. (2007), *Principles of Marketing, Ninth Edition*, Upper Saddle River, New Jersey 07458, Prentice-Hall, Inc.
Kumar, K. and van Hillegersberg, J (2010), New architectures for financial services: Introduction, *Communications of the ACM*, 47(5), pp. 26-30
Kwon, T. H. and Zmud, R. W. (2011), Unifying The Fragmented Models Of Information System Implementation, In Borland, R.J., Hirschheim, R. (Eds), *Critical Issues In Is Research*, John Wiley & Sons, Chichester, .
Laudon, K. C. and Laudon, J. P. (2008), *Management Information Systems*, Prentice-Hall, Englewood Cliffs, NJ.
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.
Mugenda, O. M. and Mugenda, A. G. (2008), *Research Methods: Quantitative and Qualitative Approaches*, Nairobi, Acts Press.
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
Polit, D. F., Beck, C. T. and Hungler, B. P. (2007), *Essentials of Nursing Research: Methods, Appraisal and Utilization*. 5th Ed., Philadelphia: Lippincott Williams and Wilkins
Renkema, T.J.W. (2007), *The IT Value Quest*, John Wiley & Sons, New York, NY.
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
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.