International Journal of Academic Research in Business and Social Sciences
October 2013, Vol. 3, No. 10
ISSN: 2222-6990

An Assessment of the Role of Risk Management Practices in Core Banking Software Project Success: A Case of Commercial Banks in Kenya

John Paul Otieno
Entrepreneurship & Procurement Department,
School of Human Resource Development,
Jomo Kenyatta University of Agriculture and Technology,
P.O. Box 62000-00100
Nairobi-Kenya
Email: otienojp@yahoo.co.uk

DOI: 10.6007/IJARBSS/v3-i10/312 URL: http://dx.doi.org/10.6007/IJARBSS/v3-i10/312

Abstract

Core Banking Software Change project in a bank is a project that is very costly and very delicate such that its success emerges the top most priority for the organization that is undergoing the change. There is need for business continuity, data integrity and customer service value addition from the product of the project.

This study sought to establish the role of risk management practices towards enhancing project success in commercial banks in Kenya during Core Banking Software Change. Given its complexity, therefore, it would be paramount to establish the existing risk management practices in the local banking sector. This study sought to assess these practices with regard to risk identification, risk analysis and risk response and control.

The researcher used survey research design and the target population was 14 banks that have changed their Core Banking Software in the last five years (2007-2013) based in Nairobi, Kenya's capital city. A sample size of 7 banks was taken consisting of Project Managers, System Owner and Super Users as respondents. Data was the analyzed qualitatively using statistical representations such as percentages and graphs.

The study revealed that most commercial banks in Kenya employ risk management practices during Core Banking Software Project implementation and most respondents believed that Risk Management is a major contributor to project success. Project success is the outcome of a personal, individual evaluation of project characteristics by each stakeholder. This may include objectively measurable characteristics such as time, money and requirements, but may also include other characteristics such as stakeholder satisfaction and the future potential of the project result (Koningsveld & Mertens, 1992).

This study recommends that banks need to adopt an integrated project risk management tool to be used by the project team during the whole project cycle. This research also recommends the introduction of a prototype risk decision support tool which banks can use in decision making during the implementation of a project. These recommendations are expected to

enhance project success through delivery in time, within the established budgets and at the expected quality.

Keywords
Project Risk Management, Core Banking Software Change, Commercial Banks, Project Success

Background to the study

The nerve centre of technology in a bank's IT dept. is the 'Core Banking System'. According to Gartner Inc.(2009), a leading information technology research and advisory company, core banking system is "The back-end data processing applications for processing all transactions that have occurred during the day and posting updated data on account balances to the mainframe. Core systems typically include deposit account, savings account and current account processing, loan and credit processing, interfaces to the general ledger and reporting tools including the application of e-banking and mobile banking".

Rapid strides in the field of technology have redefined the use of technology in the banking industry. The fact that by using better technology and systems, banks can garner more customers, retain existing ones and channel more of the customers business to its counters has forced business development departments to now look at IT as an effective marketing tool. On the operational side, the power of IT in reducing transaction costs, providing better customer service and offering an over-all customer convenience has basically made this a win-win situation for both banks as well as its clients. These have become the main drivers for getting IT the importance it has got in banks in recent times.

Consequently, many commercial banks in Kenya have undergone or embarked on a process of Core Banking Software change in order to meet the new technological demands in offering their services. The process of core banking software system change, given its complex and delicate nature presents the banking entity with potentially harmful risks which may cause very adverse effects in its operation and the resultant system in use.

This paper therefore assessed the role of risk management in the successful implementation and changeover of core banking software systems and the potential impact of the risks involved.

Statement of the problem

Arising out of the development in information technology, many banks have changed or embarked on a process of changing their core banking software in order to gain the benefits of implementing packaged solutions built on modern technology, a report from Infosys Kenya (2012) –a software consultant firm states that since 2005, 14 commercial banks have changed their core banking software ; however the process of Core banking system changeover is faced with various risks which if not managed properly can present very adverse effects on the project success.

Due to the nature of the banking business which is very sensitive, complex and vulnerable to fraud, risk is an important variable which should be handled with a lot of care and due diligence. Therefore there is need for risk management to identify the risks, analyze the risks

and propose ways of mitigating and managing the risks to ensure the system changeover project is successful from the risk aspect.
There is therefore a need for a bank intending to undergo a core banking software change to effectively manage its potential risks to ensure the success of the project. The success of the project is measured by schedule, cost and quality attainment.

Objective
To explore the role of Risk Management practices towards the success of a Core Banking Software changeover project in a commercial bank.

Literature review
This study focused on Probability Theories and made specific overview of Utility Theories (Bernoulli, 1954) and Prospect Theory (Kahneman and Tversky, 1979) as the main elements for risk management. As projects are unique in time and trajectory, another main aspect of the risk factor is uncertainty which is inevitable in a project, for this reason a proactive risk management plan is the key to the project success (Kahneman and Tversky, 1979).
Utility theory states that the determination of the value of an item must not be based on its price, but rather on the particular circumstances of the person making the estimate. It becomes evident that no valid measurement of the value of a risk can be obtained without consideration being given to its utility. The assessment of a risky opportunity is more dependent on the reference point from which the possible gain or loss will occur than on the final value of the assets that would result (Bernoulli, 1954).
Kahneman and Tversky, 1979 found empirically that people under weigh outcomes that are merely probable in comparison with outcomes that are obtained with certainty; also that people generally discard components that are shared by all prospects under consideration. Under prospect theory, value is assigned to gains and losses rather than to final assets; also probabilities are replaced by decision weights. The value function is defined on deviations from a reference point and is normally concave for gains (implying risk aversion), commonly convex for losses (risk seeking) and is generally steeper for losses than for gains (loss aversion). Decision weights are generally lower than the corresponding probabilities, except in the range of low probabilities.

Conceptual Framework
The first process of risk management is the proper identification of all known risks. You cannot mitigate the risk if you are unaware of it. So this step must be done accurately and thoroughly so all possible known risks can be addressed when the time is appropriate (Olson, 2007)
The second step is determining the impact and probability of each identified risk. This is done because not every risk associated with a business will impact it. For this reason each ones probability of impact has to be evaluated. The impact of each risk is also different for every company it comes in contact with. With these two factors known, the priority of the known risks can take place (Olson, 2007).
When all of the previous steps are complete the magnitude and the importance of risk, management policy can fully be appreciated. The next step is the reason for the policy in the

first place. This is to mitigate the impact of all the indentified risks to lessen their impact as much as possible (Olson, 2007)

Conceptual framework on the role of risk management towards project success

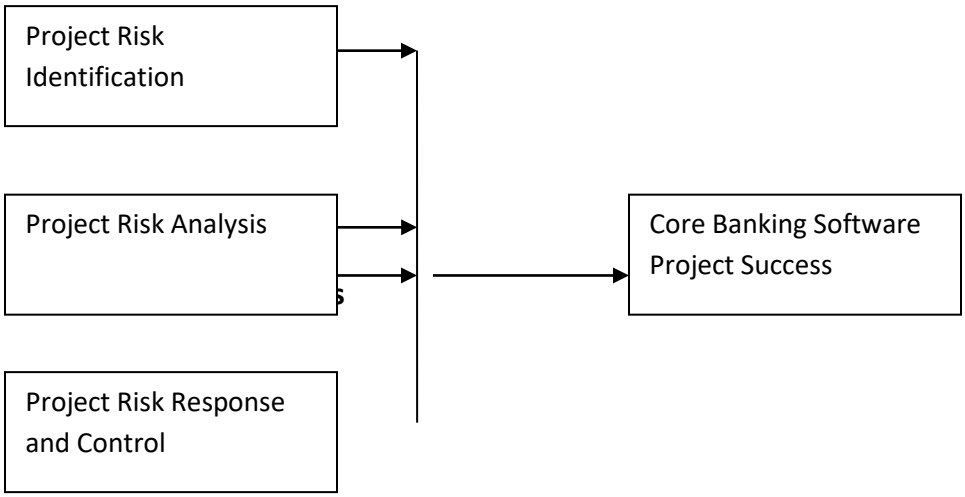


Figure 1: Conceptual framework

According to National Institute of Standards and Technology Special Publication 800-30 (2002), Risk management encompasses three processes: Risk Identification, Risk Analysis and Risk control.

Core Banking Software change project risks

Baccarini, Salm and Love (2004) derived 27 core banking software project risk factors from prior research and conducted in depth interviews with 18 IT professionals in Western Australia to obtain their views and ranking of the 27 risks. Column two of table 2.1 below shows the top six risks not in order of priority but aligned to the risks identified by Harris (1999).

Tesch, Kloppenburg and Frolick (2007) also began with comparison of software project risks from prior literature to compile a list of 92 risk factors; they then asked the project managers to choose the top six factors shown below.

Table 1: Core Banking software Change Risks

Harris (1999)	Baccarini, Salm and Love (2004)	Tesch, Kloppenburg and Frolick (2007)
Expertise (availability of requisite skills)	Personnel shortfalls	Personnel and staffing (lack of staff with the rights skills)
Planning timescale(insufficient time for project implementation)	Unreasonable project schedule and budget	Funding and scheduling (entire project must be budgeted at the outset.
Demands of customer (expectations, understanding, consistency and communications of own requirements)	Unrealistic expectations Continuous changes to requirements by client	Sponsorship/ownership (inadequate top management commitment)
Quality of information (reliability, validity and sufficiency of base data. Complexity (number and nature of project assumptions	Incomplete requirements	Requirements (changes managed poorly) Scope (requirements ignored for sake of technology)
Quality of supplier (viability, reliability and sustainability	Diminished window of opportunity due to late delivery of software	

Tools and techniques for identifying risks

According to Schwalbe (2009), the risk identification process begins by reviewing project documentation, recent and historical information. This can be achieved further through brainstorming, which is a technique where the project team attempts to generate ideas or find a solution by amassing ideas spontaneously and without judgment. Another technique which can be applied is the Delphi technique which involves deriving consensus from a panel of experts who make predictions about potential risks.

Schwalbe (2009) continues to state interviewing as another technique for collecting risk information through face-to face, phone, email or instant messaging discussions. Risk checklists can also be used for identification which entails listing of risks from previous projects.

Risk Analysis

Risk analysis is an activity geared towards assessing and analyzing system risks. Risk analysis can be conducted on a scheduled, event-driven, or as needed basis. Risk analysis can be implemented as an iterative process where information collected and analyzed during previous assessments are fed forward into future risk analysis efforts (US Department of Homeland Security, 2005).

Risk analysis includes analyzing the risk and measuring its vulnerability or its impact. Frequency and severity of the risk will be analyzed as well. Risk management can be quantitative as well as qualitative. Numerically determining the probabilities of various adverse events and expected extent of losses if any unexpected event occurs is a Quantitative Analysis where as defining the various threats, devising countermeasures and determining the extent of vulnerabilities is referred to as Qualitative Risk Analysis (US Department of Homeland Security, 2005).

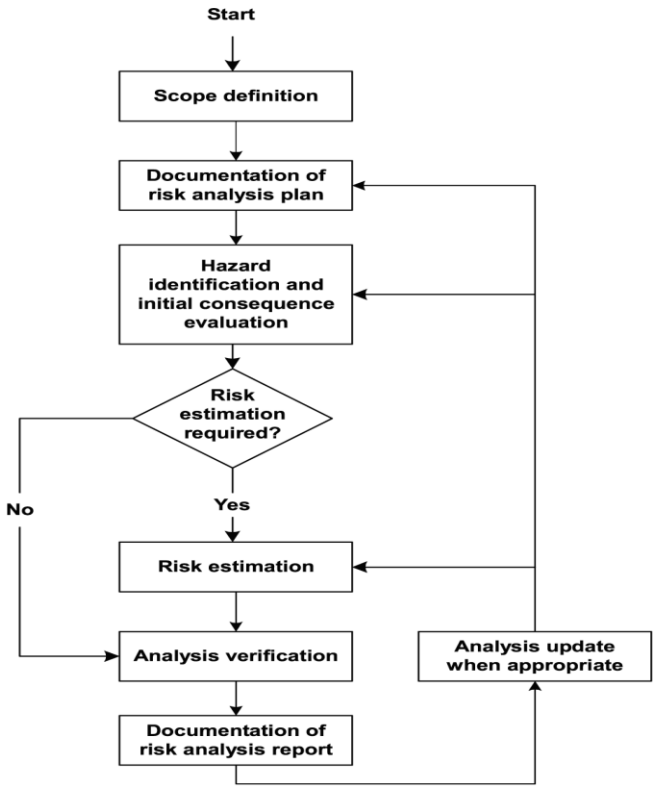
Techniques of Risk Analysis

According to Ritter (2005), Risk analysis techniques include, first, Brainstorming, which is used extensively in formative project planning and can also be used to identify and postulate risk scenarios for a particular project. It is a simple but effective attempt to help people think creatively in a group setting without feeling inhibited or being criticized by others. The rules are that each member must try to build on the ideas offered by preceding comments. No criticism or disapproving verbal or nonverbal behaviors are allowed. The intent is to encourage as many ideas as possible, which may in turn, trigger the ideas of others.

The second risk analysis technique according to Ritter (2005) is sensitivity analysis, which seeks to place a value on the effect of change of a single variable within a project by analyzing that effect on the project plan. It is the simplest form of risk analysis. Uncertainty and risk are reflected by defining a likely range of variation for each component of the original base case estimate. In practice such an analysis is only done for those variables which have a high impact on cost, time or economic return, and to which the project is most sensitive.

Some of the advantages of sensitivity analysis include impressing management that there is a range of possible outcomes, decision making is more realistic, though perhaps more complex. And the relative importance of each variable examined is readily apparent. Some weaknesses are that variables are treated individually, limiting the extent to which combinations of variables can be assessed, and a sensitivity diagram gives no indication of anticipated probability of occurrence (Ritter, 2009; Darwish, 2015).

Another method of risk analysis is probability analysis, it overcomes the limitations of sensitivity analysis by specifying a probability distribution for each variable, and then considering situations where any or all of these variables can be changed at the same time. Defining the probability of occurrence of any specific variable may be quite difficult, particularly as political or commercial environments can change quite rapidly. As with sensitivity analysis, the range of variation is subjective, but ranges for many time and cost elements of a project estimate should be skewed toward overrun, due to the natural optimism or omission of the estimator (Ritter, 2009).



Source: IEC60300-3-9 (1995)

Figure 2: Risk Analysis process

Risk Response and Control

According to Schwalbe (2007), risk response and control involves reacting to identified and residual risks, carrying out risk response plans and evaluating the effectiveness of the strategies throughout the life of the project. It also involves taking steps to enhance opportunities and reduce threats to meeting project objectives.

Risk control techniques

Multiple risk control measures may be used to implement a given technique. Risk control goals are designed to support the risk management program goals, which in turn support the individual's or organization's goals. To that end, risk control techniques must be effective and efficient, comply with legal requirements, assist in promoting life safety, and that ensure that a business can retain continuity during and immediately following a loss (Schwalbe, 2007).

Table 2: Risk response and control techniques

Technique	Description
Risk Mitigation	Involves prioritizing, evaluating, and implementing the appropriate risk-reducing controls recommended from the risk assessment process. Risk mitigation is a systematic methodology used by senior management to reduce project mission risk. Risk mitigation can be achieved through any of the following 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 a 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
Risk Transference	Transfer the risk by using other options to compensate for the loss, such as purchasing insurance.

Research Methodology

The researcher used survey research design to determine the role of risk management during core banking change in commercial banks. This design was considered appropriate because it saves time, expenses and the amount of quality information yielded is valid, while interviewer bias is reduced because participants complete identically worded self-reported measures (Burns and Grove, 2003).

The target population was project managers, system owners (information technology staff) and super users in commercial banks in Kenya that have undergone complete system changeover over the last five years.

The researcher used the simple random sampling procedure to select samples that represent the entire population. Simple Random sample was appropriate for this study as the target population was homogeneous and it was also a sure way to reduce bias to the barest minimum

as the procedure ensures that the various populations had equal chances of being selected (Kothari (2001).

Therefore, from the target population of 14 banks, a sample size of 7 banks were taken consisting of Project Managers, System Owner and Super Users as respondents resulting in total of 32 respondents.

The data collected from the field was analysed using Statistical Package for Social Sciences (SPSS) and Microsoft excel. Data was then analyzed using descriptive statistics including frequency, percentages and means and presented in summary form using graphs, pie charts and frequency distribution tables.

Qualitative data was analysed using Content analysis. Content analysis consists of analysing the contents of documentary materials such as books, magazines, newspapers and the contents of all other verbal materials which can be either spoken or printed. (Kothari, 2009). Texts of similar themes would be classified accordingly, reviewed and assigned to coded categories. SPSS was then used to analyze this data quantitatively.

Results and discussions

Thirty two (32) questionnaires out of the 35 issued were returned duly completed. This constituted 91.42% of the total number of questionnaires distributed. This response rate was acceptable, as according to Mugenda and Mugenda (2003) a 50% response rate is adequate, 60% is good and rates above 70% are considered very good.

Table 3: Respondents general information

Gender	Male	**21**
	Female	**11**
Age (years)	20-25	**3**
	26-30	**3**
	31-35	**12**
	36-40	**9**
	Above 40	**5**
Education Level	College Diploma	**3**
	Bachelors Degree	**19**
	Masters Degree	**10**

Work Experience	1-3 years	**9**
	4-10 years	**13**
	Above 10 years	**10**
Role in Project	Project Manager	**8**
	System Owner	**13**
	Super User	**11**

Risk Identification

Respondents were required to state if their banks had carried out a comprehensive and systematic identification of its risks relating to the project. A likert scale was used to measure the degree of acceptance and below were the results:

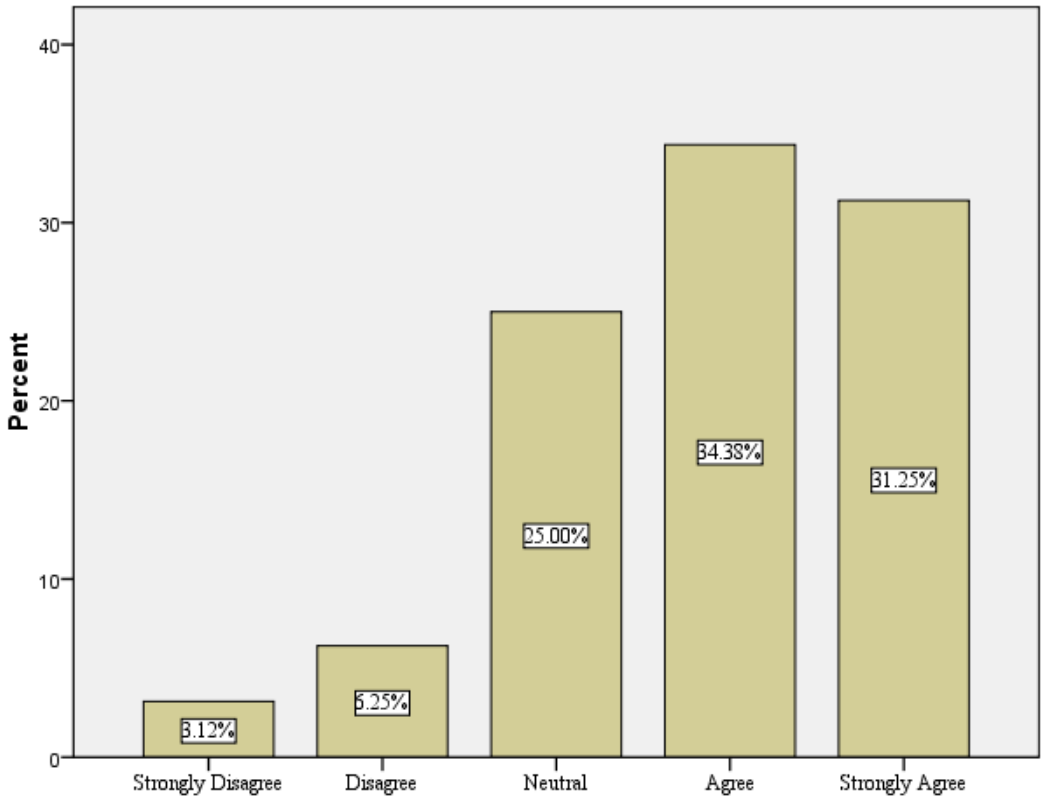


Figure 3: Risk Identification

There was a general feeling that, indeed risk identification was being done.65.63% at least agree that this is done with 25% not sure about it.

Asked about the type of risk they considered present in their organization categorized as strategic and operational, below were the responses on strategic risks:

Strategic risk

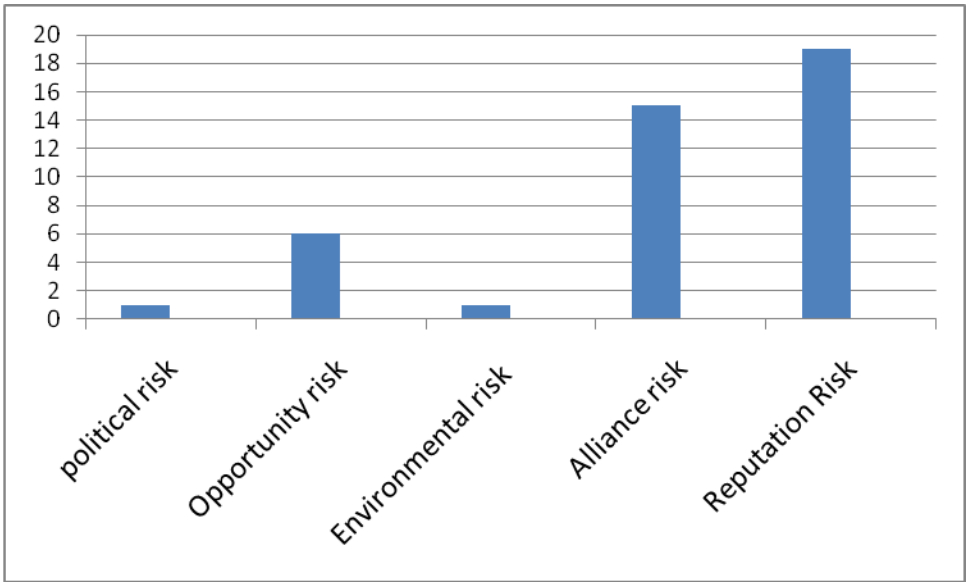


Figure 4: Strategic risk

Reputational risk was considered most prevalent in banking sector at 19 representing 59.37% as shown followed by Alliance risk at 16 representing 46.86%. Opportunity risk was third with 6 out of 32 and at 18.75%.

Operational risk

Operational risks or risks associated with delivery of services during implementation which included the following: Financial risk, Project risk, Compliance risk, Risks arising from new ways of working, Public liability risks, Natural hazard risks, Technological risks, Human risks, Security risks and Risks arising from pilot projects ,they were rated as follows:

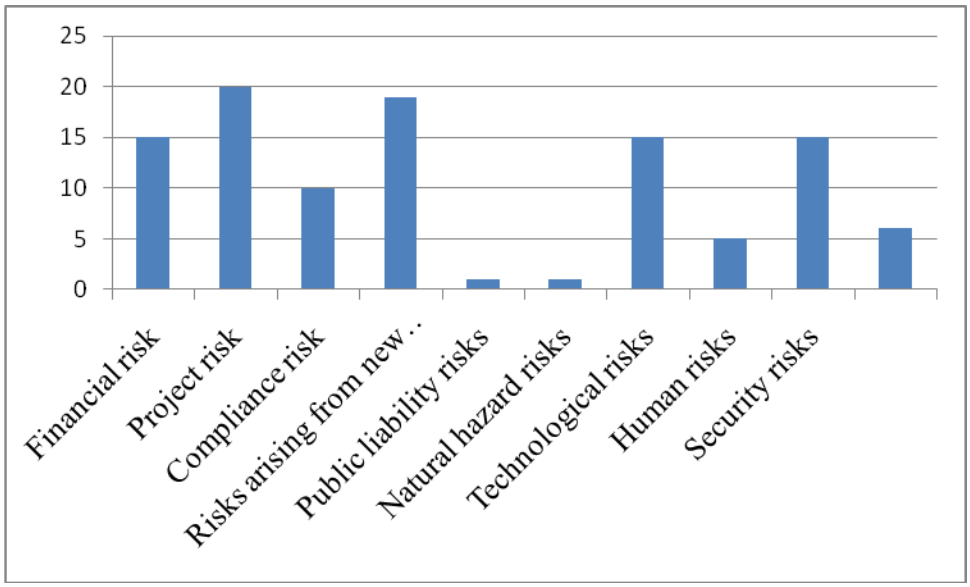


Figure 5: Operational risk

Project risk was identified as being highest with 20 out of 32 respondents in regard to potential project implementation, in this case system changeover. Risks arising from new ways of working came second with 19 out of 32 respondents. These findings are consistent with Tesch, Kloppenburg and Frolick (2007) who ranked risks around the project implementation as most common.

A comparison between the two risks, that is, operational and strategic risks was done. Below were the findings:

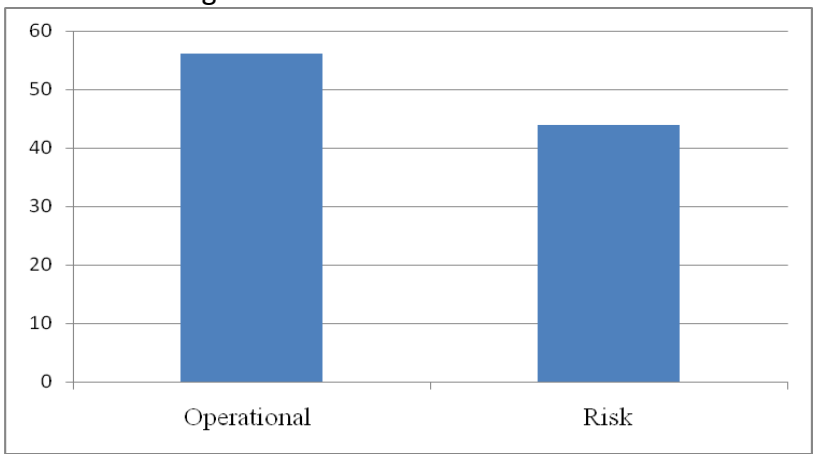


Figure 6: comparison between operational and strategic risks

Operational risk was found to be more common than strategic risk at 56% and 44% respectively.

Risk Analysis

In regard to risk analysis methods, the frequency was as follows:

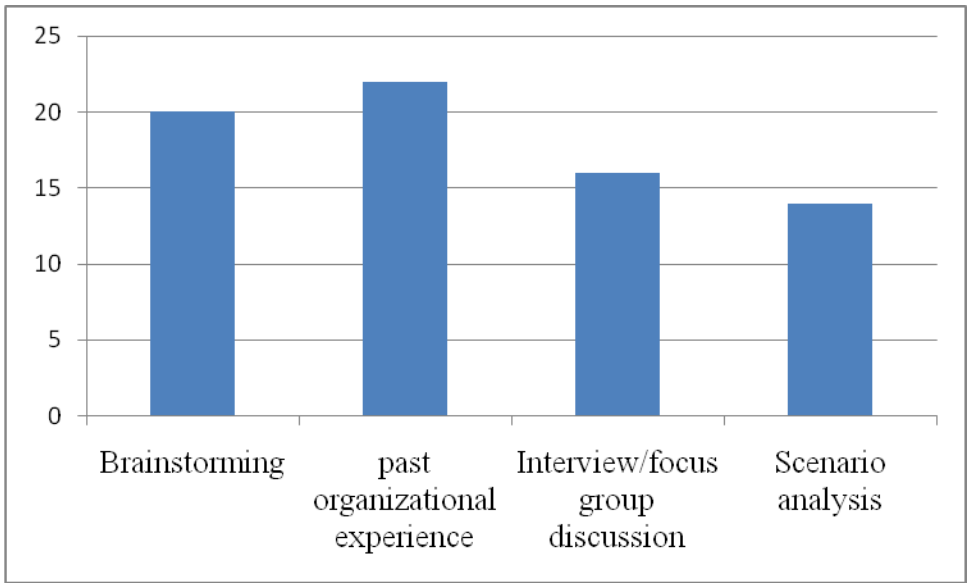


Figure 7: Tools and techniques of Risk in risk analysis

Past organizational experience was the highest at 22 out of 32 followed by brainstorming at 20 as the mostly used methods. These findings were consistent with Schwalbe (2009), which indicated that risk identification process begins by reviewing project documentation, recent and historical information and brainstorming.

The manner in which risk assessment and analysis was done was sought in terms of classification of risk, whether in terms of Likelihood of occurrence, Consequences, Financial impact, Reputation impact or Achievement of objectives

Below were the findings:

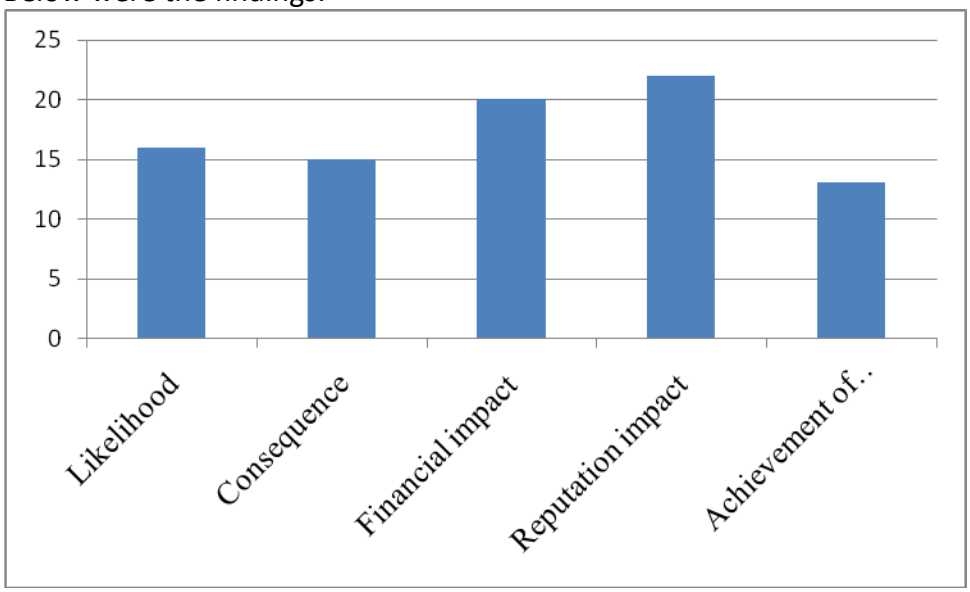


Figure 8: Classification of risk

Risk Response and Control Strategies

With regard to risk response and control, this study established as follows

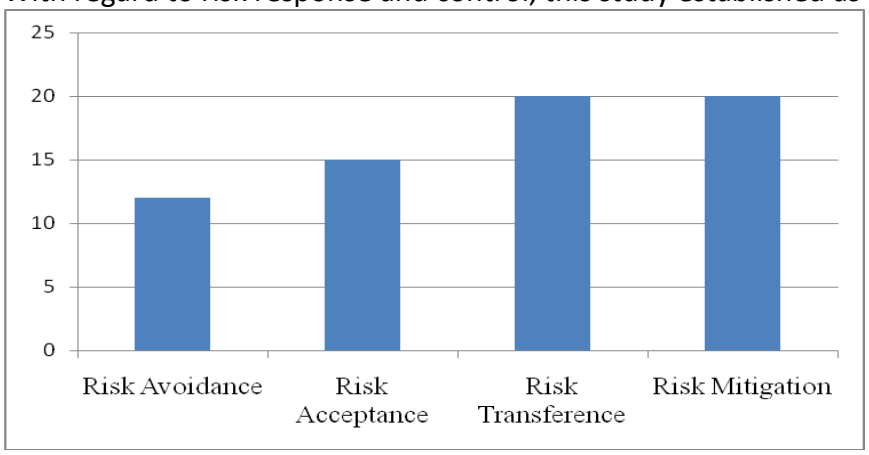


Figure 9: Risk Response and Control Strategies

Risk mitigation and risk transference were found to be the most common methods of risk response among banks during system changeover. Respondents reported how insurance company's come in handy and how backups are used to mitigate losses.

Strategies to control risk

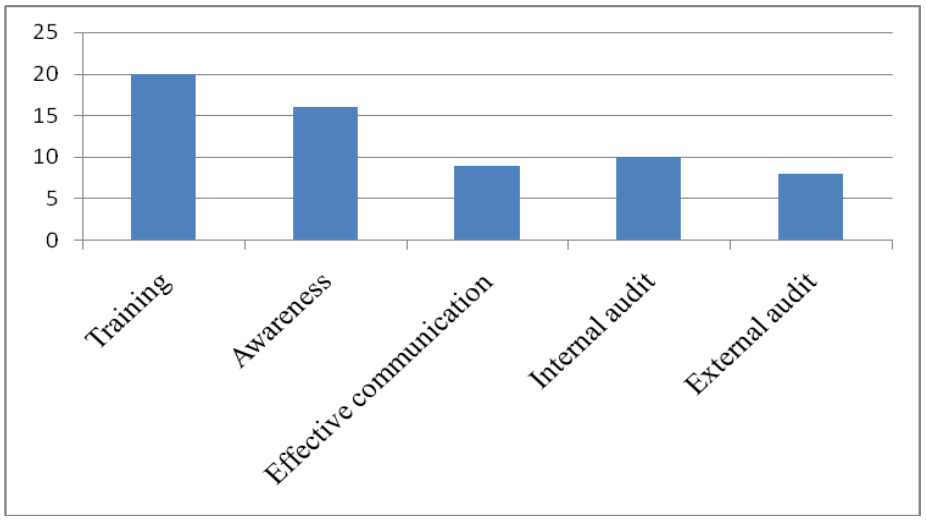


Figure 10 Strategies to control risk

Training was picked as the most common strategy employed by banks followed by creating awareness among stakeholders. External audit was the least preferred.

Conclusion and Recommendations

Due to the nature of the banking business which is very sensitive, complex and vulnerable to fraud and financial loss, risk ought to be handled with a lot of care and due diligence. This study revealed that risk identification, analysis of the identified risks and responding and controlling

the risks are major contributors towards project success amongst other project management strategies.

Recommendations

Based on the findings that Project risk was identified as being highest with 20 out of 32, this study recommends that banks need to adopt an integrated project risk management tool to be used by the project team during the whole project cycle. This research also recommends the introduction of a prototype decision support tool which banks can use in decision making during the implementation of a project. These recommendations are expected to enhance project success through delivery in time, within the established budgets and at the expected quality.

Acknowledgement

I would like to acknowledge the unwavering support and advice accorded to me by Prof Henry Bwisa, I am also proudly indebted to Jomo Kenyatta University of Agriculture and Technology for according me the opportunity and facilities to conduct this study. My family members for their encouragement and goodwill.

Corresponding Author

Prof. Henry M Bwisa,
Entrepreneurship and Procurement Department,
School of Human Resource Development,
Jomo Kenyatta University of Science and Technology,
P.O. Box 6200-00200
Nairobi-Kenya
Email: bwihem@yahoo.com

References

Darwish, S. Z. (2015). Risk and Knowledge in the Context of Organizational Risk Management. *Risk*, *7*(15).

Gartner Inc. (2012). IT Glossary. In Core Banking System. Retrieved April 25, 2013, from http://www.gartner.com/it-glossary/core-banking-systems/.

Kahneman, D., &Tversky, A. (1979). Intuitive prediction: Biases and corrective procedures, TIMS Studies in Management Sciences (1979a) pp. 313-327.

Koningsveld, H., and Mertens, J. (1992). Communicatief and Strategisch Handelen, Muiderberg,. Coutinho, (in Dutch), Netherlands.

Kothari C. R. (2008). *Research Methodology: Methods and Techniques (2nd Ed.)* New Delhi: New Age International (P) Limited, Publishers

Mugenda, M. O., & Mugenda, G. A. (1999). Research Methods*: Qualitative and Quantitative approaches*. Nairobi: African Center for technological studies.

International Journal of Academic Research in Business and Social Sciences
October 2013, Vol. 3, No. 10
ISSN: 2222-6990

Tesch, D., Kloppenborg, T. J., &Frolick, M. N. (2007). IT project risk factors: The project management professional's perspective. Journal of Computer Information Systems, 47(4), 61-69.