

THE INTERNATIONAL JOURNAL OF BUSINESS & MANAGEMENT

Risk Management Strategies and Implementation of Online Banking Technology Projects by Selected Commercial Banks in Kenya

Martha Mathenge

MBA Student, Department of Management Science, Kenyatta University, Kenya

Dr. Paul Sang

Lecturer, Department of Management Science, Kenyatta University, Kenya

Abstract:

The implementation of the online banking technology projects by commercial banks has proved to be a double edged-sword. On one had the banks in Kenya have introduced various types of online banking technology. These technologies have enabled the banks to realise significant growth in customer numbers, reduction in costs, and an increase in profits. On the other hand, the technology projects have posed a significant threat to the banks. The online banking technology projects have inherent risk. The risks include disruption of critical processes, breach of private and confidential client and employee information, and coordinated disruption of services attacks. Banks have been forced to spend approximately ten percent of the total information technology budget on dealing with the risks that accompany the use of on-line banking technology. This research purposed to determine the influence of risk management strategies on the implementation of online banking technology projects by commercial banks in Kenya. The risk management strategies that were evaluated in the study included risk assessment, risk mitigation, risk transfer, and risk acceptance. Project implementation was indicated by cost, quality, and time taken. The study was anchored by the Enterprise Risk Management Theory and Logical Framework Approach. The study adopted the descriptive research design. The study population consisted of the 39 commercial banks operating in Kenya as at 31st September 2018. The study collected data using questionnaires. The study established that risk assessment and risk acceptance strategies have a positive and statistically significant effect on the implementation of online banking projects. The effect of risk mitigation and risk transfer strategies were found to be positive but statistically insignificant.

Keywords: Risk transfer, risk assessment, risk acceptance, risk mitigation, online banking technology, cyber attack

1. Introduction and Background

Rapid changes in the field of technology have redefined the process of banking. Worldwide, banks have discovered that by using technology and systems they can attract more customers, retain existing customers, and channel more of the customer business from the counters to online platforms thus doing away with the need for the traditional brick and mortar branches (Otieno, 2013). Consequently, many commercial banks have embarked on the process of enhancing the use of technology and employing more advanced technology in their operations. Additionally, the experience of consumers with retail and communications companies that use technology to enhance the consumer experience has shaped the consumers' expectations of banks. According to Sullivan (2018), customers are becoming more digital, demanding more tech-savvy, legacy banking infrastructure. As a result of the demand for enhanced digital projects, commercial banks across the global are investing substantial amounts of money on digital platforms and projects.

Csiszar (2018) identified five main technology transformations in the banking industry globally. The first is blockchain technology which involves breaking down financial transactions into packets. These packets are encrypted to ensure that they are secured and then added to a chain of codes. Blockchain is similar to money remitted like email messages. The second is upgraded Automated Teller Machines (ATMs) with the customer being able to perform ATM transactions with their mobile phone. For example in India and Qatar, consumers use biometric authentication to access their accounts from the ATM using their smart phones. The third is more user-friendly applications (apps) this is hoped to revolutionise how the consumer interacts with the bank and its products. The fourth is automated financial services employees whereby artificial intelligence (AI) is being used to perform the duties previously done by bank employees. The AI has cognitive abilities that are used for sales, marketing, investment, wealth management, and compliance functions. The fifth is digital banking technology whereby mobile telephone technology, internet technology and other internet based platforms are used to offer banking services.

Research by Garcia (2018) indicated that commercial banks around the globe are spending billions of dollars on technology upgrades and advances. Banks have benefited greatly from the use of technology in their operations but these benefits have been diminished by the risks associated with the use of these technologies. According to Bevan, Ganguly,

Kaminski, and Rezek (2018), for many banks across the globe, these technologies form a significant part of the risks. These risks include interruption of normal and critical processes and operation, theft of customer and employee information, and blocking of access to services. Cyber security accounts for approximately 10% of total information-technology spending by commercial banks. These expenditure has been found to be growing at three times the rate of other expenditure items.

Despite these huge expenditures, the risks associated with the technology projects by commercial banks still remains a challenge. In February 2016 hackers were able to steal more than \$81 million from the Central Bank of Bangladesh by taking advantage of short-falls in the Swift financial communication network, in November 2016 \$3.1 million was stolen from 9,000 accounts of Tesco Bank; in July 2018 it was reported that two commercial banks in Kenya lost more than \$860,000 through their online banking platforms; Kenya Commercial Bank lost Ksh. 72.6 million from mobile banking and internet banking platforms due to fraud by four of its employees (Zetter, 2016; Perez, 2016; Olingo, 2018; Sunday, 2018). This raises the question of the risk management practices during the implementation of technology projects by commercial banks.

2. Research Problem

Rapid changes in the field of technology have redefined the process of banking. Worldwide, banks have discovered that by using technology and systems they can attract more customers, retain existing customers, and channel more of the customer business from the counters to online platforms thus doing away with the need for the traditional brick and mortar branches (Otieno, 2013). Consequently, many commercial banks have embarked on the process of enhancing the use of technology and employing more advanced technology in their operations. Research by Garcia (2018) indicated that commercial banks around the globe are spending billions of dollars on technology upgrades and advances. Banks have benefited greatly for the use of technology in their operations but have also become susceptible to the concomitant risks associated with these technology projects. According to Bevan, Ganguly, Kaminski, and Rezek (2018), many banks have found that these technologies are involved in more than half of their critical operational risks.

Despite these huge expenditures, the risks associated with the technology projects by commercial banks still remains a challenge. In February 2016 hackers were able to steal more than \$81 million from the Central Bank of Bangladesh by exploiting vulnerabilities in the Swift financial communication network, in November 2016 \$3.1 million was stolen from 9,000 accounts of Tesco Bank; in July 2018 it was reported that two commercial banks in Kenya lost more than \$860,000 through their online banking platforms; Kenya Commercial Bank lost Ksh. 72.6 million from mobile banking and internet banking platforms due to fraud by four of its employees (Zetter, 2016; Perez, 2016; Olingo, 2018; Sunday, 2018). It is against this background that the study hoped to evaluate the effect of risk management practices on the implementation of technology projects by commercial banks in Kenya. The study only focused on internet banking platforms.

Numerous studies have been conducted to evaluate the effect of risk management strategies on firm's performance. Alu (2013) established that mobile banking and internet banking were a major source of risks for commercial banks in Nigeria. Alu (2013) did not investigate the risk management practices that the commercial banks used when implementing the mobile and internet banking projects. This study extended the research of Alu (2013) by determining the effect of the risk management practices used by selected commercial banks in Kenya and their impact on project implementation. Mongare, and James (2017) investigated the influence of project management practices and implementation of information technology projects amongst selected commercial banks in Kenya. Mongare and James (2017) established that the banks applied risk management strategies. However, the study did not evaluate the individual components or risk management strategy nor did that study focus on online banking technology. This study aimed to fill the research gap.

3. Objectives of the Study

- To determine the effect of risk assessment on the implementation of online banking technology projects by commercial banks in Kenya.
- To establish the effect of risk mitigation on the implementation of online banking technology projects by commercial banks in Kenya.
- To assess the effect of risk transfer on the implementation of online banking technology projects by commercial banks in Kenya.
- To evaluate the effect of risk acceptance on the implementation of online banking technology projects by commercial banks in Kenya.

4. Significance of the Study

Effective risk management strategies in project management help to identify the strengths, weaknesses, opportunities, and threats. This study seeks to determine how risk management strategies affect the implementation of online banking technology projects. The findings of the study will be relevant to project managers who wish to identify and incorporate risk response strategies. The project managers will also be able to identify how the risk response strategies impact the performance of the project. The findings of the study will also be useful to policymakers as they will be able to identify the risk response strategies being used by project managers. This information will be useful when developing guidelines and policies to the risks facing the banking sector arising out of new technology. Professionals in the field of project management will be able to identify the risk management strategies that can be used when implementing

technology projects and the effectiveness of the strategies. The study will offer more information on how a critical element of project management, risk, can be mitigated against.

5. Review of Literature

5.1. Theoretical Review

5.1.1. Enterprise Risk Management Theory

This theory advocates for the management and measurement of all significant risks that the organisation faces using a holistic approach rather than managing each risk independently (Nocco & Stulz, 2006). The theory combines various risk management strategies in order to come up with a comprehensive and holistic framework. The ERM model requires that the senior management and company executive in collaboration with all the employees participate in the process of identifying, evaluating, and responding to the different types of risks that the company faces (Hallowell, Molenaar, & Fprtimato, 2013). This approach shifts the paradigm whereby only a few individuals are tasked with risk management to one where all the employees in the organisation participate in risk management.

The model maintains that the firm can enhance the risk management capacity by formulating policies that clearly stipulates the firms risk appetite and tolerance, strategic goals, and systematic process for identifying, evaluating, managing, and controlling risks (Olson & Wu, 2010). In the model there is also an emphasis on the support of risk management culture where all the stakeholders are mutually accountable and allowed to manage risks. This theory is associated with enhanced stakeholder confidence, enhanced competitive advantage, and long-term viability of the organisation (Cormican, 2015).

5.1.2 Logical Framework Approach

This approach was developed in 1969 by Rosenberg for the United States Agency for International Development (USAID). The framework provides a methodology that can be used to design, monitor, and evaluate projects. The approach is presented in the form of a 4x4 table. The events that take place during the process of project implementation namely activities, outputs, purpose, and goals are presented in the rows of the table (Fernando, 2012). Details about the project are contained in the table. Table 2.1 presents the Logical Framework Model.

Description of the Project Objectives		Objectively Provable Measures of Goal Attainment	Methods and Framework of Verification	Suppositions
Goal	What is the cumulative impact of action taken?	What are the main indicators of the overall goal?	What is the source of data for the indicators?	What external elements are required to maintain the goals in the long term?
Purpose	What are the immediate outcomes of the project?	What are the indicators that the immediate outcomes have been attained?	What are the sources of information and methods to be used to collect this information?	What are the external factors and conditions required to fulfil the purpose of the project?
Outputs	What are the pre-determined deliverable outcomes expected to attain the pre-determined objectives?	What are the elements that can be used to measure the degree to which the tasks performed achieved the pre-determined objectives?	Where will the information to measure the outcomes come from?	What are the external factors that need to present for the objectives to be fulfilled within the stipulated time?
Activities	What are the tasks to be undertaken and in what sequence will they be done so as to ensure that the pre-determined goals are achieved?	What are the internal and external resources needed to implement the identified activities?	How will progress be measured and how will the information be obtained?	What are the conditions needed for the activities to begin?

Table 1: Logical Framework Approach

Source: Schmidt (2009)

This framework provides a top to bottom model for planning project activities where the project planners start by specifying the goals of the project, the goals which are used to outline the intended achievements, identify the main activities needed to accomplish the objectives of the project, the resources required to perform each activity, and identify risks. The purpose section outlines the outcomes that the project intends to achieve for example 'improve online internet banking services'. The output section details the project intervention strategies. These might include increase number of

online banking transactions. The activities section outlines the tasks that are needed to achieve the project outputs. The activities section details that the goods and services, and processes that are needed to carry out the project activities (Goeschel, Weiss, & Pronovost, 2012).

6. Research Methodology

Similar to the approach employed by Kinyua et al. (2015) the researcher adopted the descriptive research design. Mugenda and Mugenda (2003) describe the descriptive research design as one that entails the utilisation of qualitative and/or quantitative data to test hypotheses or to provide answers to the research questions. This design allows for the characteristics of the study population to be evaluated (Kinyua et al. 2015). The target population are all the commercial banks operating in Kenya. Publications by the Central Bank of Kenya (CBK) indicate that there were forty-two commercial banks licensed to operate in Kenya as at September 2018 (CBK, 2018b). However, due to numerous challenges only 39 of the 42 licensed commercial banks were in operation as at September 2018 (CBK, 2018b). The 39 operating commercial banks are the population of the study. Given, the sample size, census sampling approach was used. The researcher obtained information from the information and technology managers of the 39 commercial banks. The information and technology managers are responsible to technology and risk management of the technology used by the bank and thus would be best placed to answer the study questions.

Primary data was used in this project. The primary data was collected using structured questionnaire (Appendix 2) to collect information. The questionnaire was developed after reviewing theoretical and empirical literature. Each question in the questionnaire was formulated to address the research questions.

7. Results and Findings

The estimation results are summarised in Table 2

	Model	Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	-9.190	2.770		-3.317	.002
	Risk Assessment Strategies	2.361	.436	.712	5.413	.000
	Risk Mitigation Strategies	.005	.187	.004	.027	.979
	Risk Transfer Strategies	.028	.209	.020	.136	.893
	Risk Acceptance Strategies	.382	.414	.130	.923	.000

Table 2: Coefficients

a. Dependent Variable: Project Implementation

Source: Study Data (2019)

The findings summarised in Table 2 indicate that risk assessment strategies have a positive and statistically significant effect on the implementation of on-line banking projects undertaken by the commercial banks sampled in this study. The findings suggest that a unit increase in the use of risk assessment strategies will result in a 2.361 increase in the implementation of on-line banking projects. These findings confirm the findings of Tadayun et al. (2012) and Junior and de Carvalho (2013) that risk assessment strategies positively affect the implementation of projects.

The $\beta = 0.005$ suggests that risk mitigation strategies have a positive effect on the implementation of on-line banking projects by commercial banks. The p-value = 0.979 suggests that the effect is statistically insignificant. These findings contradict the findings of Otieno (2013) and Bhoola et al. (2015) who established that risk mitigation strategies were the most important risk management strategies in the process of project implementation.

The coefficient of 0.028 implies that risk transfer strategies have a positive effect on the implementation of on-line banking projects undertaken by commercial banks in Kenya. The p-value = 0.893 implies that the effect is statistically insignificant. These findings contradict the findings of Junior and Carvalho (2013) and Mburu et al. (2015) that risk transfer strategies have a significant effect on the implementation of projects.

The results summarised in Table 2 suggest that risk acceptance strategies have positive and statistically significant effect on project implementation as implied by $\beta = 0.382$ and p-value 0.000. The findings suggest that a unit increase in the use of risk acceptance strategies will result in a 0.382 unit increase in project implementation by the sampled commercial banks. The findings confirm the findings of Kisk and Ukaga (2008) and Kargi (2011).

8. Discussion of Findings

The first objective of the study was to determine the relationship between risk acceptance strategies and project implementation. Overall the effect of risk assessment strategies on project implementation was found to be positive and statistically significant. Based on the findings the study can conclude that the use of risk assessment strategies namely risk identification, evaluation of risk using qualitative and quantitative techniques, adherence to central bank regulations on risk assessment, the development and management of a risk register, and the ranking of risks will result in the successful implementation of projects.

The second objective of the study was to assess the relationship between risk mitigation strategies and project implementation. The effect of risk mitigation strategies on project implementation was found to be positive but not statistically significant. These findings imply that risk mitigation measures such as the cataloging of risk mitigation strategies for each category of risk; adherence to the regulation set out by CBK on risk mitigation strategies, and; establishing a hierarchy for the approval of projects with a given level of risk do not result in greater levels of implementation of online banking technology projects by commercial banks in Kenya.

The third objective of the study was to determine the relationship between risk transfer strategies and implementation of online banking projects by commercial banks in Kenya. The study established that risk transfer strategies have a positive but statistically insignificant effect on project implementation. The findings suggest that commercial banks in Kenya do not use risk transfers strategies during the implementation of online banking technology projects.

The fourth objective of the study was to determine the relationship between risk acceptance strategies and the implementation of online banking technology projects. The overall effect of risk acceptance strategies on project implementation was found to be positive and statistically significant. Based on the findings the study can conclude that for implementation of online banking to be successful the banks need to understand and clearly define the level of risk tolerance; the risk; use sensitivity analysis to identify risk parameters that may affect the project and use the information to determine whether to accept the project or to reject; and that risk adaptive strategies be used

9. Recommendations

Based on the findings of the study, the researcher recommends to the management of commercial banks that they should enhance the use of risk identification strategies. The identification of the various risk associated with online banking projects will reduce the number of project failures. The study findings suggest that the commercial banks need to review their risk mitigation strategies and formulate strategies that have a significant effect on the risk management on project implementation. Studies have shown that risk mitigation strategies counter the chances of project failure only if they are tailored to the specific risk. Thus, the banks need to adopt risk mitigation strategies that are effective for handling risks associated with online banking technology.

The study recommends that the banks should adopt risk transfer strategies. The project risks can be shifted to different project phases in order to reduce the chances of cost and budget overruns. Additionally, the study recommends that the banks transfer portions of the risks associated with online banking projects to third parties such as insurance companies in order to lessen the financial impact. The study recommends that the banks should enhance use of risk acceptance techniques. The use of risk identification and planning should be interlinked to the risk acceptance strategies. The ability to identify and plan for risk will enable the banks to know what action to take. The actions include taking contingency measures or doing nothing except monitoring the status of the risk.

10. Recommendations for Future Studies

The study was thus limited to risk management strategies. Future studies should focus on project management strategies and how they affect the implementation of online banking projects undertaken by commercial banks. Additionally, future studies should expand the scope to include banks in the region, within the continent, and internationally.

11. References

- i. Bevan, O., Ganguly, S., Kaminski, P., & Rezek, C. (2018). The ghost in the machine: Managing technology risk. *Mckinsey & Company*. Retrieved from www.mckinsey.com/business-functions/risk/our-insights/the-ghost-in-the-machine-managing-technology-risk
- ii. Bhoola, V., Hiremath, S., & Malik, D. (2014). An assessment of risk response strategies practiced in software projects. *Australasian Journal of Information Systems*, 18(3), 161-191.
- iii. Central Bank of Kenya. (2017). *The Kenya financial sector stability report 2016*. Nairobi: Government Press.
- iv. Central Bank of Kenya. (2018a). *Annual report year 2017*. Nairobi: Government Printer.
- v. Central Bank of Kenya. (2018b). July-September 2018 Credit Survey. Retrieved from <https://www.centralbank.go.ke/reports/bank-supervision-and-banking-sector-reports/>
- vi. Federal Transit Authority. (2015). *Key factors for successful project implementation*. Retrieved from www.transit.dot.gov/regulations-and-guidance/key-factors-successful-project-implementation
- vii. Fernando, R. (2012). Getting on with it: Monitoring and evaluation in the third sector. *Risk and Regulation*. 24(4), 6-7.
- viii. Garcia, A. (2018). JPM, big banks spend billions on tech but innovations lag. *Bank rate*. Retrieved from www.bankrate.com/banking/jpm-big-banks-spend-billions-on-tech-but-theyre-still-laggards/
- ix. Goeschel, C., Weiss, W., & Pronovost, J. (2012). programs. *International Journal for Quality in Health Care*. 24 (4), 330-337
- x. Jun, G. Qiuzhen, R. & Qingguo, E. (2010). Effects of project risk planning on IT project performance focusing on a case of China vendor firms. *Project Management Journal*, 31(1), 32-43.
- xi. Junior, R., & de Carvalho, M. (2013). Understanding the impact of project risk management on project performance: An empirical study. *Journal of Technology Management and Innovation*, 8, 64-78.
- xii. Kargi, H. S. (2011). *Risk management strategies and the performance of projects by Nigerian banks* (unpublished MBA Project). Ahmadu Bello University, Nigeria

- xiii. Kinyua, E., Ogollah, K., & Mburu, D. (2015). Effect of risk management strategies on project performance of small and medium information communication technology enterprises in Nairobi, Kenya. *International Journal of Economics, Commerce, and Management*, 3(2), 1-30.
- xiv. Mongare, C., & James, R. (2017). Project management practices and implementation of information technology projects among selected commercial banks in Kenya. *International Journal of Business & Law Research*, 5 (4), 36-54.
- xv. Nocco, W., &Stulz, M. (2006). Enterprise risk management: Theory and practice. Retrieved from <https://ssrn.com/abstract=921402> or <http://dx.doi.org/10.2139/ssrn.921402>
- xvi. Olingo, A. (2018, July 7). Two Kenyan banks lose \$0.86 million to hackers in a month. *The East African*. Retrieved from theeastafrican.co.ke/business/Two-Kenyan-banks-lose-to-hackers/2560-4663272-mfv6oy/index.html
- xvii. Otieno, P. (2013). An assessment of the role of risk management practices in core banking software project success: A case of commercial banks in Kenya. *International Journal of Academic Research in Business and Social Science*, 3(10), 305-319.
- xviii. Perez, R. (2016). Tesco bank resumes services lost 2.5 million, 9,000 customers affected. *The Cyber Security Source*. Retrieved from www.scmagazineuk.com/tesco-bank-resumes-service-lost-25-million-9000-customers-affected/article/1475953
- xix. Project Management Institute (2013). *A guide to the project management body of knowledge (PMBOK) (5th ed.)*. Newton Square, PA: Project Management Institute.
- xx. Schmidt, T. (2009). *Project management made simple: Practical tools for leaders and teams*. New York: Wiley.
- xxi. Sullivan, A. (2018). 10 big financial technology trends for 2018. *The Financial Brand*. Retrieved from <https://thefinancialbrand.com/69779/financial-technology-trends-data-ai-blockchain/>
- xxii. Sunday, F. (2018, August 2018). How tech-savvy rogue bankers collude to steal your cash. *The Standard Newspaper*. Retrieved from www.standardmedia.co.ke/business/article/2001293657/how-tech-savvy-rogue-bankers-collude-to-steal-your-cash
- xxiii. Srinivasan, R., & Lohith, P. (2017). *Pilot study- assessment of validity and reliability*. Retrieved from www.researchgate.net/publication/315512816_Pilot_Study-Assessment_of_Validity_and_Reliability
- xxiv. Zetter, K. (2016). That's insane, \$ 81 million Bangladesh bank heist? Here's what we know. *Conte Nast*. Retrieved from www.wired.com/2016/05/insane-81m-bangladesh-bank-heist-heres-know/