INFORMATION TECHNOLOGY RISK MANAGEMENT IN INTEGRATED FINANCIAL MANAGEMENT INFORMATION SYSTEM IN KENYA

BY:

TRANCY KASALU

A RESEARCH PROJECT SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD OF THE DEGREE OF MASTER OF BUSINESS ADMINISTRATION, SCHOOL OF BUSINESS, UNIVERSITY OF NAIROBI

NOVEMBER, 2016

DECLARATION

This research project is my original work and has not been presented for a degree award in any other university.

……………………………….. ……..……………………….

Signed Date

Trancy Kasalu

D61/71323/2014

This research project has been submitted with my approval as university supervisor.

………………………………….. …………………………………….

Signed Date

Joel K. Lelei

Department of Management Science

School of Business

University of Nairobi

DEDICATION

I dedicate this project to my lovely Mum, Angelina Kasalu and the entire Kasalu’s family for their moral support and continuing encouragement.

ACKNOWLEDGEMENTS

I would like to acknowledge my Supervisor Mr. Joel K Lelei for his support and guidance. His advice has made this whole research project successful.

My special thanks goes’ to IFMIS staffs who took time to respond to my questionnaires.

TABLE OF CONTENTS

LIST OF FIGURES

ACRONYMS

CBK	**:**	Central Bank of Kenya
GoK	**:**	Government of Kenya
ICT	**:**	Information Communication Technology
IFMIS	**:**	Integrated Financial Management Information System
IMF	**:**	International Monetary Fund
PFM	**:**	Public Financial Management
RBR	**:**	Re-Engineering For Business Results
SCOA	**:**	Single Chart of Accounts
USAID	**:**	United States Agency for International Development
WB	**:**	World Bank

ABSTRACT

This study investigated information technological risk management associated with integrated financial management information system (IFMIS) in Kenya. IFMIS is not a new phenomenon in Kenya. Both the public and private sector have adopted IFMIS. Due to poor implementation of the system and other challenges, the users of IFMIS have experienced many problems. IFMIS system has complex features which come up with risks, security and reliability issues that have an impact on efficient cash management. The purpose of the study therefore was to investigate information technological risk management associated with IFMIS. To achieve its purpose, the study used the following three objectives to: establish the information technological risks associated with IFMIS; establish measures for mitigating IT risks associated with IFMIS application and to determine effectiveness of measures for mitigating IFMIS information technological risks. The main theoretical perspective of the study was Contingency Theory. The study adopted descriptive research and data used was primary which was collected by use questionnaires and analyzed by coming up with means and standard deviation .The population for this study was comprised of all staffs in IFMIS department in National treasury. The study concluded that the major IT risks in IFMIS is system breakdown and the most used measure to counter the IT risks in IFMIS is changing passwords regularly and the most effective measure used in IFMIS to counter the IT risks is use of antivirus to control the virus.

CHAPTER ONE
INTRODUCTION

1.1 Background of the Study

Developing countries and countries in transition over the past years have undertaken key steps to computerize major government operations mostly in the field of Public Financial Management (PFM). Among them has been the introduction and implementation of the IFMIS which computerizes and automates all main areas of the budget making and execution as well as all accounting operations across the institutions of government (Diamond & Khemani, 2005).

A strong implemented IFMIS can lead to economic growth (Brar, 2010). IFMIS ensures that the government and all its organizations can raise, manage and use all public resources in a transparent, accountable and efficient way with the aim of enhancing efficiency to improve service delivery (Ajayi & Omirin, 2007). IFMIS supports management reporting, making policy decisions and helps in coming up with financial statements which can be audited. In Kenyan government IFMIS has lend to computerization of all major process of public financial management starting from budget preparation, to budget execution and finally budget reporting (Lianzuala & Khawlhring, 2008).

IFMIS as a management tool can enable management in controlling aggregate spending as well as the deficit; also it helps management in prioritizing expenditure to attain efficiency as well as transparency in resources allocation (Barata & Cain, 2001). Integrated Financial Management Information System has been adopted as the main driver to effective public service provision as well as for wealth and work creation.

1.1.1 IFMIS Components

Integrated Financial management information system (IFMIS) is an information system used to keep track of financial operations in a business and encapsulates it, into financial information. It can be referred as an accounting system designed to function according to organizations provisions (Casals, 2009). A government IFMIS consists of core and non-core components which are integrated through an interface. The main core component is General ledger where every transaction is posted. All transactions are simultaneously posted in general ledger while others are posted in the sub-modules appropriately. Other core components of IFMIS include cash management, commitment control, accounts payable and accounts receivables. Beside the core modules, IFMIS can support or interface with other modules according to its functionality (Diamond & Khemani, 2005).

1.1.2 IT Risks

IT risks are the potentiality for unplanned events involving a failure or misuse of IT to threaten an organization's objectives, with the business consequences enterprise must change the way they manage it (Westerman & Hunter, 2007). Effective risk management process are essential for a success of an IT security platform (Casals & Associates, 2004). Risk management process of an organization should aim at the protection of the organization in order to achieve its objectives and mission and not aiming at protecting its assets only. Hence risk management is not only a technical function for IT experts to perform but it's also a major concern for the management.

Benefits realized from use of Information Technology can't be under estimated, even though there are risks which are come up with the use Information Technology. These risks issues can be divided in to two categories. The first category views risk in terms of "computer hacking, virus, system failures and access control" hence in preventing these risks means identifying those threats, evaluating their possibility of occurring hence coming up with measures to counter them. The second category deals with cost-justify solution (Sjoberg &Fromm, 2001). These IT risks can be managed by well-trained IT experts.

1.1.3 IT Risks Countermeasures

There are several measures which can be undertaken to mitigate the IT risks defending on their nature. Unauthorized access to computer system can be mitigated by use of passwords and user ID, hence triggering the locking of a user ID after several attempts of inputting wrong passwords. Passwords also should have minimum length and should expire after certain duration; this will prevent a third party from guessing a password to access a system or computer.

Firewalls are also another mechanism for preventing unauthorized access to systems (Stoneburner et al., 2002).

According to Sjoberg et al., (2001) loss of power or hand drive breakdown can result to a loss of files; this can be mitigating by ensuring that there is continues back-up of copies hence copies can be accessed in case of loss of original ones.

1.2 Research Problem

Use of Information Technology in public finance systems can result to resource accountability and transparency hence acting as tool to curb corruption (Chene, 2009). In the past years, developing countries and countries in the transition have put more efforts towards the computerization of the government procedures, with the most focus on public financial management (PFM) (Gallagher, 2007). This effort led to introduction of IFMIS among other systems. IFMIS computerizes and also automates main process of accounting operations and budget execution across government bodies (Gijselinckx & Devetere, 2007). In developing countries sound IFMIS can help government control their finance's as the operations can be done in transparency and accountable manner. It can act as a tool to eliminate corruption and fraud and also reduce political discretion (Davenport & Brooks, 2004).

Recent and available literature on IFMIS shows that related studies carried out so far have mainly focused aspects of IFMIS systems development, design, management, monitoring and evaluation, implementation as well as sustainability. Bartel (2006) discovered online procurement have failed because most institutions tend to resist change, lack in adequate technology and also lack human resource capability. This was on his study "Integrated Financial Management Systems: while Gallagher (2007) in his study on building fiscal infrastructure in post-conflict societies discovered that ineffective project coordination, lack of high level commitment, loose project design and planning are factors behind fail of IFMIS. In developing countries IFMIS is adopted as major component behind public financial reforms. IFMIS in developing countries are not successful despite the fact that more resources are allocated on them as they are faced by many challenges of institutional, political, technical and operational nature (Greta et al., 2011).

IFMIS has enabled efficient and prompt access to reliable financial data which has helped in expediting government operations, strengthening of government financial controls, raising the process of budget making to higher levels of accountability and transparency and improving the provision of government services among others (GoK, 2011).

Locally several studies about IFMIS have been carried out. According to Musee (2011) IFMIS has not been fully adopted due to sabotage, resistance from users and also lack of management support. He also established that the capacity and technical knowhow is very low as the systems are implemented in hurry and also users are not well trained or not trained at all on the use of the system. Kandi (2012) found out that IFMIS influences the impact of internal control systems on the financial performance.

Despite the fact that several studies have been carried on IFMIS, no research has been carried to evaluate information technological risk management associated with IFMIS. There is therefore a need for such a study to be carried out to investigate and document information technological risk management associated with IFMIS. This study should therefore answer these questions so as to realize its objectives; what are the information technological risks associated with IFMIS? What are the measures for mitigating information technology risks associated with IFMIS application? How effective are the measures for mitigating IFMIS information technology risks?

1.3 General Objective of the Study

The main objective of this study was to investigate the information technological risk management associated with IFMIS.

1.4 Specific Objectives of the Study

The study was guided by the following specific objectives:

i. To establish the information technological risks associated with IFMIS.

ii. To establish measures for mitigating IT risks associated with IFMIS application.

iii. To determine effectiveness of measures for mitigating IFMIS information technological risks.

1.5 Justification and Significance of the Study

This study is very important as it investigated information technological risk management associated with IFMIS. It is envisaged that the findings, recommendations and conclusions from the study will be of importance in the following ways: It is expected that the study, by coming on with the conclusion from the data collected, related literature and practical examples will catalogue and avail information on best practices for the development, design, implementation, monitoring and evaluation as well as governance of IFMIS.

It is also envisaged that policy makers will make use of the findings of this study to come up with practical mechanisms, policies and strategies for enhancing information technological risk management in IFMIS. Literature in this field is limited, therefore this study will help in availing information that can expand and enrich the existing body of knowledge. Available literature has also shown that very little empirical research has been undertaken in particular area of study. This lack of an in-depth research in this particular area has created a gap in the analyses that have been done on policy studies so far. This study therefore seeks to fill the knowledge gap by availing literature with recommendations for programming, policy development and further research.

CHAPTER TWO
LITERATURE REVIEW

2.1 Introduction

Literature review accounts for what is known and published on a certain topic by accredited scholars and researchers. This section starts with introduction followed by theoretical framework then the review of literature on research conducted on risks, measures and effectiveness of measures taken to mitigate IT risks. Finally the chapter provides the conceptual framework.

2.2 Theoretical Framework

This research used Contingency Theory to buttress its writings and answer the research questions. The contingency theory currently provides an important framework for the study of organizations (Donaldson, 2001). Propounded by Fred Fiedler, it postulates that there is no best way to lead a company, organize a corporation or to make decisions. There are numerous internal and external constraints that will change what really is regarded as the best way to manage a given situation (Fiedler & Chemers, 1967). In other words, the best course of action depends upon the situation at hand. Fiedler alleged that there exist direct relationship between the characteristics and effectiveness of a leader. According to Fiedler, leadership should change according to the circumstances, as some leadership skills can be used in times of crisis and other in different situations (Palmer & Dunford, 2002). Contingency theory alleges that there exists no one best way to manage an organization and therefore a leader should be in position to come up with the best way according to the situation to manage an organization in order to achieve its objectives. According to Donaldson (2001) some important contingencies in organizations include technology, consumer interest groups, suppliers and distributors, government, customers and competitors and unions.

2.3 The concept of Integrated Financial Management Information System

Integrated Financial Management Information System (IFMIS) is an “automated system that is used for public financial management. It interlinks budgeting, planning, management and control, expenditure, accounting, audit and reporting” (GoK, 2011). It is a financial management information system that keeps track of all financial activities and summarizes them in to financial information. Apart from performing accounting functions, IFMIS can be configured to operate in different environments according to the specifications of the environment (Diamond et al., 2005).

The functionality and scope of IFMIS varies across different countries, even though sub-systems are more or less the same; they include “budgeting, accounting, cash management, debt management and other related core systems of the treasury” (Miranda & Keefe, 2008). Besides these core subsystems, some countries have expanded the system by adding non-core subsystem such as procurement management, tax administration, pension and social security systems, asset management, human resource and pay roll systems. Other modules have also been added to support the core modules (Miranda & Keefe, 2008).

In general terms, IFMIS can be referred as the use of information and communications technology (ICT) in financial operations in order to support budget and management decisions, fiduciary responsibilities and in the preparation of financial statements and reports. In the government circles, Integrated Financial Management Information System is precisely the automation of all activities of public financial management (PFM). The automation process starts from budget preparation all the way to its execution and also the automation of accounting and reporting .This has been implemented in ministries, government institutions, departments, spending agencies and other public sector operations (GoK, 2011).

2.4 IT Risks

Use of IT has increased steadily as every organization is investing heavily on it. This has been necessitated by the benefits which come with the use of Information Technology. There are risks which come with the use of IT and which many organizations are facing since many organizations today relay on use of information system. The major risks of IT are the lack of necessary skills and Knowledge to use the systems as well as lack of experience. Technology is also changing with a very high rate, and in order for the organization to keep the pace of the same it has to do continuous training of the staff which is costly. This issue of technology change again has brought a threat as technology advances it means that organizations are continually exposed to systems frauds and hackings. If organizations doesn’t come up with an n effective mitigating measures it can end up failing to achieve t its goals and objectives (Merna & Al-Thani, 2008).

Rainer and et al.,(1991)on their studies on “Risk analysis for information technology” classified risk in to three categories; “ physical threats which are threats resulting from equipment failure, power interruption, contaminants in the air, weather, humidity, fire, destruction or damage to facility or equipment by humans, death or injury to key personnel and personnel turnover”. The second category is Unauthorized physical or electronic access risks, which are risks resulting from “microcomputer theft, theft of data, disclosure and modification of data, hackers, virus, EDI fraud, phantom nodes on network, voice mail fraud and software piracy”. And finally the third category being authorized physical or electronic access.

According to Taylor and Fleming (1999), one of the main risks of implementing integrated financial systems is the fact that different fragmented agencies and their managers brought together by integrated system become, in a sense, "lame ducks." There is therefore a need to create a single integrated agency.

Another major risk is the collapse of existing independent systems which may be caused by poor implementation of IFMIS or inconsistent in data sharing among the different components of the system. This can be mitigated through proper testing of the independent modules at each stage of integration. Vickery et al., (2003) while contributing to the same also point out the long and slow pace of transition is also a risk which may cripple processes in the affected entities almost bringing operations to a standstill. This can be mitigated by making sure that there is effective work plan which includes all details of the transition.

According to Taylor and Fleming (2001) Management should establish ways of dealing with challenges which brought about by the integrated agency. Integrated agencies can bring about staff dislocation and changing of culture; if these challenges are not dealt with effectively then they will interfere with the performance of the agencies.

Countries in transition Economies face the risk when comes to the implementation of IFMIS, as they have to move to integrated supervision model. A previous study by Vickery et al., (2003) Skills mix should be reevaluated and the old structure should be established with new one which will lead to maintenance of the previous practices.

IFMIS also faces the security risk through hacking and denial of service and this may affect efficient access and provision of services to customer. Other security risks reported include sabotage and fraud involving these systems. This can be mitigated by strengthening the security infrastructure where these systems are running (Stern, 2002).

2.4.1 Measures for Mitigating IT Risk

An organization must come up with measures to mitigate IT risks, as these IT risk might cause an organization from achieving its objectives. The responsibility to ensure this mechanism are put in and adhered to lies with the management. Management must come up with preventive measure to mitigate or prevent risks from occurring. Some of the preventive measures include; setting up of computer centers, data input controls and security devices. The preventive measures are selected according to the risks (Lye & Wing, 2005).

Preventive measures can never be effective and therefore organization's management must come up with containment measures which can detect and limit the effects of the risks which might by-pass the control measures. Such plans include dual capacity in telecommunication and computer networks, reconciliation procedures which can detect errors and contingency plans in case of major disasters (Schechter, 2004).

The main aim of the IT security policy is to come up with a framework that can be used to implement security and also come up with control measures. The information provided by the computerized systems its the major key behind IFMIS operations and there the infrastructure which supports it must be protected from the risk. This is by ensuring that it is protected from corruption, unauthorized access, and breach of confidentiality which might be accidental or deliberate and also from destruction (Embretson & Hershberger, 2009)

According to Bartel (2009) IFMIS security has been compromised a lot, as its information security policies have also been compromised. IFMIS Security systems must ensure the following objectives among others are achieved; Confidentiality- This is ensuring that data is not disclosed or accessed by unauthorized individuals; Integrity- This is ensuring that data is consistency by preventing unauthorized creations, alterations and destruction; Availability-This ensuring that those who are supposed to access a certain information can access it; Authorized-This ensuring that only authorized users can be authorized to access the system and that systems cannot be used by unauthorized persons (Bartel ,2009).

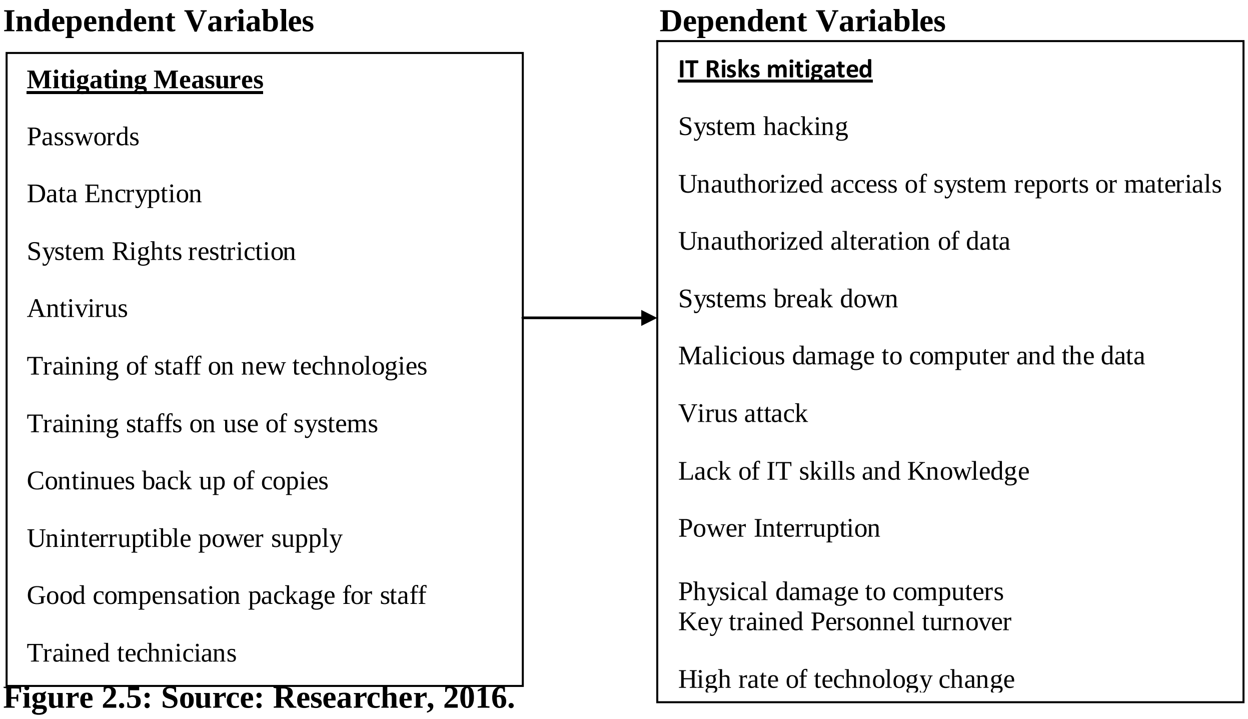
It is the responsibility of organizations management to do internal audit by reviewing, monitoring and testing control systems every day to ensure that they are effective. Also management should implement regular programs of independent tests and control procedures for the security comprising of inspectors, consultants and auditors. These programs should be in position to identify risks before they have already affected the organization. The level of the risk should determine the frequency and depth of audit tests in an organization (Schechter, 2004).

Risk identification occurs in different levels in the organization in most cases being in application level, organizational level and the inter-organizational level. Most of the risks identified at the application level are risks which occur as a result of technical failure or as result of implementation failure. These risks include both internal and external threats. Internal threats are threats such as unauthorized access of the system which can result to system abuse while external threats are threats which occur or come from the organizations environment and they include natural disasters, competitors, hackers and computer viruses. The second risk identification occurs at the organizational level, these accounts for the effects of IT in all functional areas. The main focus here is strategic risks which once occurs might hinter an organization from achieving competitive advantage. Risks can also originate from the potential countermeasures, in order to control these the management needs to do risk monitoring (Bandyopadhyay et al. 1999).

2.5 The Conceptual Framework

A conceptual framework comprises of ideas and principles obtained from different and related fields of research and used to structure a researcher's presentation (Reichel & Ramey, 1987). A well-structured conceptual framework it's important as it helps a researcher come up with meaningful findings. Framework is viewed as a starting point of reflection for research and the context. Through framework, the research can clearly explain the study hence making it easy to be understood by the reader. A Conceptual framework brings about researcher's understanding of the variables of the study and how they relate. Researcher uses conceptual models to show the relationship of the dependent and independent variables of the study either through graphs or diagrams (Mugenda & Mugenda, 2006). According to Kothari (2003), a variable is value which can change according to the condition and which can take qualities of quantitative values. A dependent variable is it's the value which the researcher observe during the study, in other words it's the outcome variable. The values of dependent variable can't be changed as they are the one that are being predicted and whose variation it's the main aim of the study. The independent variables are the values which manipulated during the study .They can also be referred as the predictor or explanatory variables. These variables can be changed and the ones that explain the change or variation in dependent variable (Alison, 1996).

In this study, independent variables of the conceptual framework were "Mitigating measures" and "IT risk being mitigated" as the dependent variables as shown in Figure 2.5. This study used conceptual framework in order to answer the research questions.



Independent Variables

Mitigating Measures

Passwords

Data Encryption

System Rights restriction

Antivirus

Training of staff on new technologies

Training staffs on use of systems

Continues back up of copies

Uninterruptible power supply

Good compensation package for staff

Trained technicians

Dependent Variables

IT Risks mitigated

System hacking

Unauthorized access of system reports or materials

Unauthorized alteration of data

Systems break down

Malicious damage to computer and the data

Virus attack

Lack of IT skills and Knowledge

Power Interruption

Physical damage to computers
Key trained Personnel turnover

High rate of technology change

Figure 2.5: Source: Researcher, 2016.

2.6 Chapter Summary and Gaps in Literature

In this chapter, research on what is known about information technological risk management associated with IFMIS has been presented and summarized under the following subheadings: the concept of Integrated Financial Management Information System, IT Risks, and Measures for mitigating IT risks and effectiveness of risk measures on IT risks. However, despite extensive studies conducted in this area, there is no empirical literature information technological risk management associated with IFMIS. This study was conducted in order to fill that gap.

CHAPTER THREE
RESEARCH METHODOLOGY

3.1 Introduction

This chapter deals with the approaches the researcher applied to collect the data for the study. Specifically it includes; research design, study population, sampling design, data collection mechanisms, data collection procedure and data analysis procedure.

3.2 Research Design

The study used descriptive research, this was preferred because it explains the situation well and this helps in avoiding bias when collecting the data hence reducing errors in data interpretation. This is achieved as the descriptive study answers the "What" questions (Cooper & Schindler, 2006).

3.3 Study Population

A population consists of all elements in which researcher make inferences in his study (Creswell, 2004). In this research the population consisted of all staff in IFMIS department in National Treasury. Both technical and business sections IFMIS staff were involved in this study.

3.4 Data Collection

This study used primary data collected using questionnaires which were administered through "drop-and –pick later" method. The questionnaires were divided in to Section A and Section B. Section A contained respondent's background information while Section B contained IT risks, IT counter measures and effectiveness of IT counter measures. The respondents were all staffs in IFMIS department.

3.5 Data Analysis

Questionnaires were referenced then tabulated response or items from it to make the data actionable. After administration of questionnaires the mass raw data collected was systematically organized in order to facilitate analysis. Data related to respondent's background was analyzed by coming up with Frequencies and percentages. In order to achieve the research objectives which are; to establish the information technological risks associated with IFMIS; to establish measures for mitigating IT risks associated with IFMIS application and to determine effectiveness of measures for mitigating IFMIS information technological risks, data was analyzed coming up with mean and standard deviation and results presented in tables. This was necessitated by use of SPSS.

CHAPTER FOUR

DATA ANALYSIS,INTERPRETATIONS AND DISCUSSIONS

4.1 Introduction

This chapters reports analysis in relation to research objectives which are; To establish the information technological risks associated with IFMIS, to establish measures for mitigating IT risks associated with IFMIS application and to determine effectiveness of measures for mitigating IFMIS information technological risks. The chapter includes detailed reports of the analysis of primary data, their presentations, interpretation and discussion of the findings.

The chapter is divided in two section; Section one which deals with General information and Section two which deals with IT risks associate with IFMIS, Measures for mitigating IT risk associate with IFMIS and Effectiveness of measures for mitigating IFMIS IT risks.

4.2 Response Rate

The questionnaires distributed were 40, and among them 30 were duly filled, returned and analyzed. This represents a 75 % response. Response rate of 50% or more it's adequate, this is according to Mugenda and Mugenda (2003). Also according to Babbie (2004) response rate of about 60% is considered to be good and that of 70% is considered to be very good hence acceptable to be analyzed and published. Hence the response rate of this research which is 75% is considered adequate in coming up with conclusions.

Table 4.2 Response Rate

Response	Frequency	Percentage
Returned	30	75 %
Unreturned	10	25 %
Total	40	100%

4.3 General Information

Analysis of general Information was done from the questionnaires, in this respect respondents were asked to provide their general information like gender and age as while as general information about their working such as; Years of service with IFMIS, their specialization and job tittle/designation. This information was essential as it provided background information of the respondents.

4.3.1 Gender

Respondents were asked to indicate their gender. The data collected was analyzed; and the results are as shown in the Table 4.3.1

Table 4.3.1 Gender

Gender	Frequency	Percentage
Male	18	60%
Female	12	40%
Total	30	100%

Male respondents were 60% while female respondents were 40%.This shows that both genders were involved in the research even though the male respondents were more than the Female respondents. This could be attributed to the fact that Male are more in government sectors than females.

4.3.2 Age

Data on age was also collected and analyzed; the results are shown on the Table 4.3. 2

Table 4.3.2 Age

Age in years	Frequency	Percentage
18-25	2	6.7 %
26-30	3	10 %
31-35	8	26.7 %
36-40	5	16.7 %
41-45	7	23.3 %
46-50	4	13.3%
Above 50	1	3.3%
Total	30	100 %

Majority of the staffs follow under the age gap of 31-35 years with 26.7 % .The minimal age gap is above 50 years with only 3.3 %. This shows that various age group were involved in the research.

4.3.3 Years of Working in IFMIS

Respondents were required to indicate the years of service with IFMIS. The data was analyzed and results presented as shown below in Table 4.3.3

Table 4.3.3 Years of Working with IFMIS

Years of Service in IFMIS	Frequency	Percentage
Less than 1 year	7	23.3 %
1-5	15	50 %
6-10	7	23.3 %
Over 10 years	1	3.4 %
Total	30	100 %

Majority of the staffs have worked with IFMIS for 1-5 years representing a percentage of 50 %, this means that respondents have good experience of working with the system hence being in a good position to give the information to achieve the research objectives. The respondents who have worked with IFMIS for less than a year are 23.3 %.

4.3.4 Area of Specialization

Respondents were required to indicate whether they belong to Technical or Business section of the IFMIS. Data was analyzed and the results are as shown in the Table 4.3.4

Table 4.3.4: Area of Specialization

Area of Specialization	Frequency	Percentage
Technical	20	66.7 %
Business	10	33.3 %
Total	30	100 %

IFMIS department it's divided into two sections, Technical and Business. From the analysis majority of the respondents were from Technical section with 66 % while minimal was from Business with 33.3 %. This shows that the two sections in IFMIS were presented.

4.3.5 Job Designation/Job Title

Respondents were asked to indicate their job designation or job title. Data was analyzed and the results are as shown in the Table 4.3.5

Table 4.3.5 Job Designation /Title

Job Designation/ Job Title	Frequency	Percentage
Finance Officer	3	10 %
Accounts Officer	2	6.7 %
Human Resource Officer	1	3.3 %
Procurement Officer	2	6.7
ICT Officer	15	50 %
Projects Officer	4	13.4 %
Head Business	1	3.3%
Head Technical	1	3.3 %
Other	1	3.3 %
Total	30	100 %

The highest response were from ICT officer with 50% which is in technical section, the other 50 % response came from the Business section represented as Finance officer, Accounts Officer, Human Resource Officer, Procurement Officer and Projects Officer. This shows that all Officers in the IFMIS were presented.

4.4 IT Risks Associated with IFMIS

The first objective sought to establish the information technological risks associated with IFMIS. The respondents here were to select from a scale where; 1-no extent; 2-little extent; 3-moderate extent; 4-large extent; 5-very large extent. Analysis was done by obtaining mean and standard deviation. Mean score corresponding with the scale was; below 1.5 no extent; 1.5 but <2.5 little extent; 2.5 but <3.5 moderate extent; 3.5 but < 4.5 large extent; 4.5 but <5.5 very large extent.

Table 4.4 IT Risks

Risks	1-No extent	2-little extent	3-moderate extent	4-large extent	5-very large extent	Mean	Standard Deviation
System hacking	12	9	2	6	1	2.2	0.630
Unauthorized access of system reports or materials	10	7	7	3	3	2.4	0.661
Unauthorized alteration of data	10	6	7	5	2	2.4	0.652
System break down	3	3	4	9	11	3.7	0.668
Malicious damage to computer and the data	14	7	4	3	2	2.0	0.642
Virus attack	2	9	7	7	5	3.1	0.612
Lack of IT skills and Knowledge on security measures	7	4	10	2	7	2.9	0.730
Power Interruption	2	5	4	11	8	3.6	0.730
Physical damage to computers	9	10	4	4	3	2.4	0.664
Key trained Personnel turnover	5	11	5	6	3	2.7	0.632
High rate of technology change	5	4	13	8	0	2.8	0.515

The highest mean is 3.7 which represents System break down while the lowest mean is 2.1 which represents System hacking. This shows that system break down occurs in large extent while system hacking occurs in little extent.

4.5 Measures for Mitigating IT Risks Associated with IFMIS IT Risks

The Second objective sought to establish measures for mitigating IT risks associated with IFMIS application.

The respondents here were to select from a scale where; 1-no extent; 2-little extent; 3-moderate extent; 4-large extent; 5-very large extent. Analysis was done by obtaining mean and standard deviation. Mean score corresponding with the scale was; below 1.5 no extent; 1.5 but <2.5 little extent; 2.5 but <3.5 moderate extent; 3.5 but < 4.5 large extent; 4.5 but <5.5 very large extent.

Table 4.5 Measures to Mitigate IT risks

Measures to mitigate IT Risks	**1-No extent**	**2-little extent**	**3-moderate extent**	**4-large extent**	**5-very large extent**	**Mean**	**Standard deviation**
Changing Passwords regularly	0	5	0	4	21	4.3	0.565
Use of Firewalls	0	3	4	10	13	4.1	0.490
Encryption of data	1	6	4	11	8	3.6	0.556
System Rights restriction	2	3	1	14	10	3.9	0.590
Training of staff on new technologies	0	7	4	12	7	3.6	0.549
Training staffs on security awareness	2	5	4	11	8	3.6	0.624
Continuous update of Antivirus	2	3	4	7	14	3.9	0.642
Continues back up of copies	2	5	6	4	13	3.7	0.468
Use of Uninterruptible power supply	3	5	8	2	12	3.5	0.716
Good compensation package for staff	7	10	5	1	7	2.7	0.740

The highest mean is 4.3 which represents changing passwords regularly while the lowest mean is 2.7 which represents good compensation package for staff. This shows that changing passwords regularly as measure to counter IT risks associated with IFMIS has been used in large extent while offering staff good compensation package occurs in moderate extent.

4.6 Effectiveness of Measures for Mitigating IFMIS

The third objective sought to determine effectiveness of measures for mitigating IFMIS information technological risks.

The respondents here were to select from a scale where; 1-no extent; 2-little extent; 3-moderate extent; 4-large extent; 5-very large extent. Analysis was done by obtaining mean and standard deviation. Mean score corresponding with the scale was; 0 but < 1.5 no extent; 1.5 but <2.5 little extent; 2.5 but <3.5 moderate extent; 3.5 but < 4.5 large extent; 4.5 but <5.5 very large extent.

Table 4.6 Effectiveness of Measures

Effectiveness of Measures	**1-No extent**	**2- little extent**	**3-moderate extent**	**4-large extent**	**5-very large extent**	**Mean**	**Standard deviation**
Security awareness	2	5	9	8	6	3.3	0.591
Retaining of staff	4	9	7	4	6	2.9	0.680
Data accuracy	2	4	5	11	8	3.6	0.609
Data availability	1	4	7	7	11	3.7	0.597
Data integrity	2	3	5	12	8	3.7	0.589
Data confidentiality	1	4	5	8	12	3.8	0.598
Data completeness	1	5	6	8	10	3.7	0.604
Data accessibility	1	6	4	10	9	3.6	0.606
Data reliability	2	4	6	9	9	3.6	0.623
Data Timeliness	2	3	6	10	9	3.7	0.603
Effective control of virus	1	4	4	4	17	4.1	0.629

The highest mean is 4.1 which represent Effective control of Virus while the lowest mean is 2.9 which represent Retaining of staff. This shows that Effective control of Virus has been achieved at large extent. While retaining of staff has been achieved at moderate extent.

4.7 Discussions of the Results

In order to achieve the first objectives of the study which was; to establish the information technological risks associated with IFMIS the mean and the standard deviation was calculated. The highest mean was 3.7 which represents System break down. This indicated that the major IT risks in IFMIS is System Break down. However the previous literature on IT risks indicated that the major IT risks are the lack of necessary skills and knowledge to use the system.

The second objective of the study was; to establish measures for mitigating IT risks associated with IFMIS application. This was achieved through calculation of mean and standard deviation. The highest mean was 4.3 which represents changing passwords. This means changing of password regularly has been the most applied measure to counter IT risks in IFMIS. This conforms with the previous literature review on Measures to mitigate IT risks which showed that changing of passwords has been used most.

The third objective was to determine effectiveness of measures for mitigating IFMIS information technological risks. Which was realized by calculating mean and standard deviation. The highest mean was 4.1 which represent Effective control of Virus. This indicates that control of virus as a IT risk has been effectively controlled.

CHAPTER FIVE

SUMMARY ,CONCLUSION AND RECOMMENDATIONS

This chapter finalizes the study by providing the summary of key findings, conclusions and recommendations which are aligned with the specific objective of the study. The study was conducted on IFMIS department in National treasury. The response rate was 75 % which represents 30 responses from possible 40 responses.

5.2 Summary

The current study was aimed at investigating the information technological risk management associated with IFMIS. This was demonstrated by the mean score of responses .The findings indicated that the most IT risks in IFMIS is system breakdown. This was indicated by the value with the highest mean score of 3.7. This shows that's system breakdown occurs in large extent. The least occurred IT risk was system hacking with 2.1 mean score.

The study also sought to establish to establish measures for mitigating IT risks associated with IFMIS application. This was also demonstrated by the mean score of responses. The findings indicated that changing passwords as most used method to mitigate IT risks in IFMIS. This was indicated by the value with the highest mean score which was 4.3. This indicated that changing passwords as a measure to counter IT risks associated with IFMIS was used in large extent. Offering good compensation package for the staff proved to have been used in moderate extent with a mean score of 2.7.

Finally the study sought to determine effectiveness of measures for mitigating IFMIS information technological risks. Which was achieved through use of mean score responses. The findings indicated that the most effective control of IT risks in IFMIS is control of Virus. This was represented by a mean score of 4.1 which proves that IFMIS had achieved effective control of antivirus. This was achieved in the higher extent. Retaining of the staffs was proved to be least achieved with a mean score of 2.9.

5.3 Conclusions

Based on the objectives and the findings of the study the following conclusions can be made; There are several IT risks which are associated with IFMIS and among those IT risks system breakdown is major risk while system hacking is the least.

IFMIS department has employed several measure to counter the IT risk among those measures changing passwords regularly is most used while offering good compensation packages to staff is least used measure to counter the IT risks associated with IFMIS.

Measures employed to mitigate the IT risk associated with IFMIS have been effective. The most achieved it's the effective control of antivirus while the least achieved it's the retaining of IFMIS staff.

5.4 Recommendations

Based on results, findings and conclusion the following conclusion was recommended. The IFMIS department should conduct system checks to avoid system breakdown which is the major IT risks in IFMIS.

IFMIS is used by many organizations especially the state corporations and the counties, this means when the systems breaks a large population of users its affected hence the need to come up with a separate server which can be used in case of the main system break down.

5.5 Limitations of the Study

Some respondents did not complete and return questionnaires and this was a challenge. There was also a problem accessing some data as it was highly controlled as a government asset. Additionally implementation of IFMIS in the Kenyan government is recent and therefore there was limited lessons learned so far as well as limited focus at the moment in the area around risk management.

5.6 Suggestions for Further Studies

A study on how to achieve effective control of system breaks down on IFMIS should be conducted and also a progressive study needs to be conducted around the same area as the IFMIS use grows in Kenya. Additionally due to the difficulties in accessing data, some of the reports on implementation of IFMIS in Kenya should be availed on the government data portal for ease of access by research and interested parties.

REFERENCE

Ajayi, C.M., & Omirin, S. P. (2007). Key Issues in Information Systems Management.

Baker, T.L. (1994). Doing Social Research (2nd Edn.). New York: McGraw-Hill Inc.

Brar, P. (2010). IFMIS in Africa: Some key issues. In Presentation for the World Bank/East Afritac Conference on IFMIS, Mombasa February (Vol. 15, p. 2010).

Chêne, M. (2009). The Implementation of Integrated Financial Information Management Systems (IFMS). Retrieved August, 4, 2015.

Creswell, J. W., & Clark, V.L.P. (2007). Designing and Conducting Mixed Methods Research.

Khemani, P., & Diamond, M. J. (2005). Introducing Financial Management Information Systems in Developing Countries (Epub) (No.5-196). International Monetary Fund.

Donaldson, L. (2001). The Contingency Theory of Organizations. Sage.

Elliott, J. (2005). Using narrative in social research: Qualitative and quantitative approaches. Sage.

Fiedler, F. E., & Chemers, M. M. (1967). A theory of leadership effectiveness.

Gallagher, M. (2007). Building Fiscal Infrastructure in Post-Conflict Societies. Washington, DC:USAID(November).

Gijselinckx, C., & Develtere, P. (2008). The Co-operative Trilemma: Cooperatives between market, state and the civil society. Working Papers on Social and Co-operative Entrepreneurship WP-SCE, 08-01.

GOK (2011). Integrated Financial Management Information System (IFMIS) IFMIS Re-Engineering, From Modular, to Full Cycle End–To-End Processes, Strategic Plan 2011-2013

Tromp, K., & Kombo, D. K. (2006). Proposal and Thesis writing. An Introduction. Nairobi: Paulines Publications.

Kothari, C. R. (2004). Research methodology: Methods and techniques. New Age International.

Miranda, R. and T. Keefe (2008). "Integrated Financial Management Systems: Assessing the State of the Art", Government Finance Review, pp. 9-13.

Mugenda, O. M. (1999). Research methods: Quantitative and qualitative approaches. African Centre for Technology Studies.

Mugenda, O. M., & Mugenda, A. G. (2012). Research methods dictionary.

Palmer, I., & Dunford, R. (2002). Out with the old and in with the new? The relationship between traditional and new organizational practices. The International Journal of Organizational Analysis, 10(3), 209-225.

Patton, M. Q. (2002). Qualitative interviewing. Qualitative research and evaluation methods, 3, 344-347.

Ritchie, J., Lewis, J., Nicholls, C. M., & Ormston, R. (Eds.). (2013). Qualitative research practice: A guide for social science students and researchers. Sage.

World Bank's Public Financial Management (PFM) Reform database, materials on PFM automation and IFMIS: http://web.worldbank.org/wbsite/external/projects/extfinancialmgmt/0,,contentMDK:21475540~iscurl:Y~menuPK:3914586~pagePK:210058~piPK:210062~theSitePK:313218,00.html.

Taylor, M., & Fleming, A. (1999). Integrated financial supervision: lessons from Northern European experience. World Bank. Available at http://info.worldbank.org/etools/docs/library/50180/TaylorFleming_1999.pdf (last accessed on 3rd September 2016)

Dhillon, G., & Backhouse, J. (1996). Risks in the use of information technology within organizations. International Journal of Information Management, 16(1), 65-74.Available at http://www.sciencedirect.com/science/article/pii/0268401295000623 (last accessed on 11th September 2016)

Sjöberg, L., & Fromm, J. (2001). Information technology risks as seen by the public. Risk Analysis, 21(3), 427-442. Available at http://www.dynamit.com/lennart/pdf/it%20risks%20risk%20analysis%202001.pdf (last accessed on 12th September 2016)

Vickery, S. K., Jayaram, J., Droge, C., & Calantone, R. (2003). The effects of an integrative supply chain strategy on customer service and financial performance: an analysis of direct versus indirect relationships. *Journal of operations management*, *21*(5), 523-539. Available at http://www.sciencedirect.com/science/article/pii/S0272696303000627

Rainer Jr, R. K., Snyder, C. A., & Carr, H. H. (1991). Risk analysis for information technology. *Journal of Management Information Systems*, *8*(1), 129-147. Available at http://www.paul-hadrien.info/backup/LSE/IS%20490/risk%20analysis%20for%20IT.pdf (last accessed on 13th September 2016)

APPENDIX 1: RESEARCH QUESTIONNAIRE

PART A: GENERAL INFORMATION

1. What is your gender?

   Male [ ]   Female [ ]

2. Indicate your age category:

   18-25years [ ]

   26-30 years [ ]

   31-35 years [ ]

   36-40 years [ ]

   41-45 years [ ]

   46-50 years [ ]

   above 50 years [ ]

3. Years of service/working period with IFMIS in National Treasury (Tick as applicable)

   Less than 1 year [ ]

   1-5 years [ ]

   6-10 years [ ]

   Over 10 years [ ]

4. Indicate your area of specialization:

   Technical [ ]   Business [ ]

5. Please specify your designation /job tittle ……………………………………….

SECTION B: INFORMATION TECHNOLOGICAL RISK MANAGEMENT ASSOCIATED WITH INTEGRATED FINANCIAL MANAGEMENT INFORMATION SYSTEM

IT risks associated with IFMIS

6. To what extent have you faced each of the following IT risks in IFMIS? Indicate using the scale; **1-no extent; 2-little extent; 3-moderate extent; 4-large extent; 5-very large extent**

Risks	**1**	**2**	**3**	**4**	**5**
System hacking					
Unauthorized access of system reports or materials					
Unauthorized alteration of data					
System break down					
Malicious damage to computer and the data					
Virus attack					
Lack of IT skills and Knowledge on security measures					
Power Interruption					
Physical damage to computers					
Key trained Personnel turnover					
High rate of technology change					

Measures for Mitigating IT Risk Associated with IFMIS

7. To what extent have you applied each of the following measures for Mitigating IT Risk in IFMIS? Indicate using the scale;

   1-no extent; 2-little extent; 3-moderate extent;

   4-large extent; 5-very large extent

Measures to mitigate IT Risks	**1**	**2**	**3**	**4**	**5**
Changing Passwords regularly					
Use of Firewalls					
Encryption of data					
System Rights restriction					
Training of staff on new technologies					
Training staffs on security awareness					
Continuous update of Antivirus					
Continues back up of copies					
Use of Uninterruptible power supply					
Good compensation package for staff					

Effectiveness of Measures for Mitigating IFMIS IT Risks

8. To what extent have you achieved each of the following outcomes as a result of risk mitigating measures applied on IFMIS IT risks? Indicate using the scale;

   1-no extent; 2-little extent; 3-moderate extent;

   4-large extent; 5-very large extent

Effectiveness of Measures	**1**	**2**	**3**	**4**	**5**
Security awareness					
Retaining of staff					
Data accuracy					
Data availability					
Data integrity					
Data confidentiality					
Data completeness					
Data accessibility					
Data reliability					
Data Timeliness					
Effective control of virus					

THANK YOU FOR YOUR TIME AND PARTICIPATION