INFORMATION TECHNOLOGY POST IMPLEMENTATION PRACTICES AND OPERATIONAL RISK MINIMIZATION IN PUBLIC HOSPITALS IN KENYA

RUGENDO K. KAMAKIA

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

UNIVERSITY OF NAIROBI

OCTOBER, 2014

STUDENT'S DECLARATION

This is to certify that this research project is my original work and has not been submitted for the award of any degree in any other university. No part of this project may be produced without the prior permission of the author and/or University of Nairobi.

_____ _____

Rugendo Kego Kamakia Date

Reg. No. D61/69131/2011

This project has been submitted for examination with my approval as University Supervisor.

Signed: _____ _____

Dr. Muranga Njihia Date

Chairman, Department of Management Science, University of Nairobi

ACKNOWLEDGEMENTS

I must start by thanking the Almighty God who inspired me into venturing in a new area of study after many years as a professional accountant. Many thanks go to the management of public hospitals and the Ministry of Health for creating an environment for me to birth the idea of researching in the area of risk and for making it possible for me to obtain information from their institutions.

I am very grateful to my supervisor Dr. Muranga Njihia for technical and methodological guidelines, and the constructive comments offered to this study. I also thank my moderator Mr. Joel Lelei for his useful assistance in moderating the study.

Special thanks go to my able assistants Salmon Otiato and Jason Oyalo for their invaluable logistical and facilitational support. Finally, let me take this opportunity to sincerely thank my class mates, colleagues, family and friends who have supported and encouraged me throughout this course.

DEDICATION

I would like to dedicate this study to my lovely wife Florida G. Rugendo and our dear children, who have tirelessly given me every necessary support during my studies. My prayer is that they be blessed abundantly.

ABSTRACT

This study was carried out to establish the relationship between IT post implementation practices and IT operational risk minimization among the public hospitals in Kenya. The study had three objectives: To establish the IT post implementation practices in public hospitals in Kenya; to identify the existing IT operational risks in public hospitals in Kenya; to determine the relationship between IT post implementation practices and IT operational risk minimization among public hospitals in Kenya. The study used the cross-sectional survey. A census survey was carried out in all hospitals in the selected six counties and data collected from the respondents through a closed questionnaire. Data collected for objectives one and two was analyzed using mean scores while data for objective three was analyzed using multiple regression analysis. The study revealed that IT systems have been in use for an average of 3 years in the public hospitals. The results show that due to the inadequacy of IT post implementation practices adopted, the level of exposure of IT systems to IT operational risk is high; there is lack of hospital-wide IT policies and procedures and finally there is an inverse relationship between IT post implementation practices and IT operational risk minimization in public hospitals. The study recommends that hospitals implement comprehensive policies and procedures to guide IT operations, and address IT security and control issues. It is also recommended also that IT system changes and updates be documented. Finally, it is recommended that the hospital management take advantage of the accumulated knowledge on IT systems to provide leadership towards enacting appropriate institutional risk strategy and risk management framework.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ACRONYMS AND ABBREVIATIONS OF TERMS

BBA: British Bankers' Association

BCBS: Basel Committee on Banking and Supervision

COSO: Committee of Sponsoring Organizations

ERP: Enterprise Resource planning

HMIS: Hospital Management Information Systems

ICT: Information and Communication Technology

IIF: Institute of International Finance

ISACA: Information Systems Audit and Control Association

ISDA: International Swaps and Derivatives Association

ISO: International Organization for Standardization

IT: Information Technology

MIS: Management Information System

MNC: Multinational Corporations

MOH: Ministry of Health

PwC: PricewaterhouseCoopers

RMA: Risk Management Association

SME: Small and Medium Enterprises

SPSS: Statistical Package for Social Sciences

CHAPTER ONE: INTRODUCTION

1.1 Background of the Study

Enterprise risk is a risk that encompasses all major risks faced by a business firm (COSO, 2004). This risk can be classified according to its nature and thus may include pure risk, speculative risk, strategic risk, reputation, legal, operational risk and financial risk. Enterprise risks can also be classified according to the source of the risk: Internal, strategic and external risks. Internal risks are risks that are caused by factors within the organization that can be controlled such as the risk of employee misconduct, systems and technology failures while strategic risks are risks taken on by an organization in the pursuit of value (for instance the risk associated with an investment in developing a new computerized production system) and external risks are largely beyond its control An example is the risk of impact from a natural disaster like an earthquake, economic and political factors (Thuku, 2012).

These days a growing number of companies devote a significant portion of their management effort discussing risk and risk management. However a vast majority of organizations have made very little effort to ascertain the risk profile of their companies and this in effect means that they have not put any structures in place to address the risks.

1.1.1 Operational and Information Technology Risk

Operational risk is part of enterprise risk and results from the firm's business operations; such as from services offered using computer systems that hackers may break into (COSO, 2004). Shevchenko (2010) notes that in 1990's there was no widely accepted definition of operational risk. Often, operational risk was defined as any risk not categorized as market or credit risk. Some defined it as the risk of loss arising from various types of human or technical error.

BBA, ISDA, RMA and PwC (1999) came up with the first universally accepted definition of operational risk which was later affirmed by the BCBS (2004). They defined operational risk as the risk of loss resulting from inadequate or failed internal processes,

people and systems or from external events. It is the risk of loss arising from the potential that inadequate information systems; technology failures, breaches in internal controls, fraud, unforeseen catastrophes, or other operational problems may result in unexpected losses or reputation problems. The BCBS (2004) adds that such operational risk captures business continuity plans, environmental risk, crisis management, process systems, people related risks and health and safety, and IT risks.

Abolhassani and Moghaddam (2008) (as cited in Akbari, 2012) while appreciating the definition of operational risk by BCBS (2004) opinioned operational risk is the risk of failure and lack of efficiency in personnel, technology and working process. This appears to be in line with the definition used by Credit Suisse Group (as quoted by IIF and McKinsey & Co., 2011) that operational risk is the risk of adverse impact to business as a consequence of conducting it in an improper or inadequate manner and may tangibly manifest itself in the likes of business disruption, control failures, errors, misdeeds or external events. The BCBS (2004) definition of operational risk has been adopted or adapted by many firms, but it is just one of many possible definitions that can be used. This study adopts this definition.

The importance of operational risk has been highlighted recently with spread of IT applications which has brought about new problems for organizations. Any failure of the IT systems was give rise to a major element of operational risk known as IT risk (and includes such threats as business interruption, disaster recovery, business and information security, data backup and protection, business license compliance and social media used (Jammal, 2011). BCBS (2006) adds to this list human error, external fraud by intruders, obsolescence of applications and machines, availability, performance, reliability issues, mismanagement and natural disasters.

Kitheka (2013) defines IT risk as the risk of failure or malfunction of the IT applications and infrastructure used to support a company. He goes ahead and identifies the relevant elements of IT infrastructure as: network and user management, configuration management, system performance and capacity, IT service request, service level and

helpdesk management. The study adopts this definition but also includes data backup and protection and disaster preparedness, license compliance and IT security.

1.1.2 Information Technology Operational Risk Minimization

By the very nature of project management there will always be uncertainty. Whether it's small or large, complex or simple, every project has risk. It is the job of managers to do their best to minimize the risk in projects (Bogue, 2005). The first step to risk minimization is to identify all risks that are possible in the organization and consider all internal and external factors that could give rise to the risks. The next step is to evaluate the risk based on its probability and impact to the organization's operations. The risks are then prioritized and managed by putting in place measures to control them and having mitigation strategies for those risks that can't be controlled. During the implementation phase all risks must be constantly monitored in accordance with the risk assessments.

The greatest cost of an IT system implementation occurs long after the initial development and deployment is over, when the system enters its support and maintenance phase of its life cycle. Adopting good practices will therefore reduce the long term operational cost and associated risks (Murphy, 2010).

1.1.3 Information Technology Post Implementation Practices

Acquiring advanced technologies does not necessarily lead to success. Firm's performance critically depends on how these technologies are implemented. Successful implementation of these technologies requires among other things a human resource strategy to develop the necessary worker skills and engage them in the process (Hornstein, 2008). Karimi (2006) argued that IT system implementation depends on many factors affecting the project's pre-implementation, implementation and post implementation stages. He identified these factors as comprising four elements: data classification, management controls, operational controls and technical controls. During each implementation stage the organization is required to put in place practices that address these elements and as a consequence there was minimal disruption of the IT systems. This study was concern itself with the practices adopted by organizations to

guide IT implementation during the post implementation stage. For this study post implementation is the stage after the project is handed over to the client by the vendor.

Kimwele (2013) argues that there is evidence from his survey to suggest that despite numerous technical guides and principles there is no recognized, standard approach at an organization-wide level to help in addressing these IT challenges and suggests that SMEs could develop and adopt appropriate IT security standards and policies, identify IT security roles and responsibilities, create IT security awareness, put in place data recovery measures, and protect organizational assets. He also suggests that laps in practice accounts for the serious IT security challenges faced by SMEs in Kenya.

Asangansi (2013) argues that the implementation of HMIS has become a major challenge for researchers and practitioners because of the significant proportion of failure of implementation efforts. He states that researchers have attributed this significant failure of HMIS implementation, in part, to the complexity of meeting with and satisfying multiple (poorly understood) logics in the implementation process. It is also possible that there could be a relationship between the failures and the implementation practices adopted.

The IT systems implementation process is complex and as such requires careful consideration of the organizational context (Galdwin et al, 2003)). National polices and guidelines are expected to be reflected in the plans of the implementing institutions, but prioritized to reflect the context. The sad thing is that some of the government organizations examined are not aware of the national ICT policy and have continued to implement ICT systems without referring to the policy (KACCA, 2008).

New risk categories such as operational, strategy and reputational risk are highlighted as new critical focal areas by Deloitte (2012) for an organization and more importantly it was reported that risk management programs have not been quite effective in these areas. Implementing a successful operational risk discipline was require significant changes in corporate cultures, senior management understanding of and commitment to a robust internal risk management structure (BITS, 2004).

1.1.4 Information Technology Post Implementation Practices and IT Operational Risks

Post implementation practices affect the risk levels of an organization. What the company does or does not do after an IT system is put in place greatly affects the success or failure of the system. Obviously, failure leads to IT risk from malicious actions, man-made and natural disasters, or inadvertent errors made by users and so forth. Over the past few decades, IT applications have become more susceptible to these risks because of the wide spread usage of computers, the interconnectivity of these computers, and rapid development of Internet applications (Badie, 2011). Risk is also fueled by the lack of appropriate practices that creates an enabling environment for implementing IT systems.

ISACA, 2006 (as quoted by Önal, 2006) puts it that since IT is now central and widely used, organizations will continue to be exposed to operational risks related to the use of IT such as virus attacks, breakdown of infrastructure, unauthorized access to data, performance problems, system and infrastructure contingency. A survey carried out by Taub (2002) found that 81 percent of organizations feel they are vulnerable to a serious operational incident.

Without proper IT Governance, IT systems can lose integrity with serious implications on performance and can also result in breach of client confidentiality (Makau, 2010 as quoted by Munene, 2009). Galdwin et al (2003) and KACCA (2008) noted that some organizations were implementing ICT systems without reference to any policy. As a consequence organizations are exposed to serious vulnerability to information systems security violations.

Experience has shown that IT operation risk exposure of an organization increases with the used of IT. The extent of the exposure depends on the post implementation practices adopted after the project is handed over by the vendor. Research shows that IT operational risk is fueled by lack of appropriate practices to guide IT implementations and worse by the fact that some organizations do not know what to do.

1.1.5 Public Hospitals in Kenya

Kenyan hospitals can be divided into different facility types under public, faith based, private and non-governmental. Public hospitals scan be distinguished from the rest of the facilities by having been officially gazetted and "taken-over" by the government and placed under the Ministry of Health (MOH), or are under the Prisons, local authorities, Armed Forces, academic, parastatal or the Constituency Development Fund. The hospitals under MOH are categorized into five levels with each level providing different services to the public. The five categories are: provincial general hospitals, district hospitals, sub-district hospitals, health centres and dispensaries. There are approximately 6,150 hospitals in Kenya of which 41% are public.

The health sector in Kenya has a multiplicity of health information systems – manual, computer and web-based. There is little co-ordination between systems and much duplication of data and effort. Yet according to the MOH these systems rarely yield the quality of information necessary for the planning, programme and resource monitoring, and performance-based review that the health managers require (MOH, 2010).

The key institutions that influence ICT policy formulation and implementation in Kenya public institutions include the Ministry of Information and Communications; ICT Authority and Communications Commission of Kenya. The ICT Authority is mandated with marketing Kenya as an ICT market leader and coordinating the provision of public sector shared service.

1.2 Statement of the Problem

IT operational risks result from improperly performing ICT operations and lead to loss of computer assets, increased risk of fraud, loss or theft of data, privacy violations and business disruption (Straub & Welke, 1998); This risk implies that internal processes, people and systems are controlled inadequately (BCBS, 2004). These findings provoked interest to find out if hospitals in Kenya are facing these risks and what internal and other controls are in place to minimize these types of risks.

Though the government develops ICT guidelines and policies for hospitals to follow the guidelines are in general terms and do not prescribe the implementation details which are left to the hospitals (Goldwin et al, 2003). Waema (2010) et al studied the key challenges facing the ICT sector in Kenya and pointed out that there is poor implementation of these policies by government institutions. A study by Woods (2009) concluded that the central government and MOH policies are key variables in the management of IT implementations in public hospitals. This study intends to find out how the public hospitals adopt government guidelines for minimizing IT post implementation risks.

Ernst & young (2012) survey in United States quoted that 65% of the surveyed organizations reported that they would have trouble recovering from system-wide computer failure before it caused significant disruption to their business. Since the study was in USA, a study may be required to find out how organizations in Kenya would recover from a serious computer failure and ensure the IT systems are restored to their original state.

Kimwele et al (2005) found evidence to suggest that IT security policies are not widely adopted by Kenyan SMEs and according to Makumbi et al (2012) small business owners in Kenya are unclear on how to safeguard their businesses from IT risks that come with the increased reliance on IT. A gap exists for researchers to find out how hospitals in Kenya protect their IT assets and what IT risks they face.

Kimwele, 2005; Nicolaou, 2008; Gladwin et al, 2008 and Hughes, 2006 focused on the IT implementation process itself and pre-implementation factors as well as risk management process. They did not carry a study on IT post implementation practices or IT operational risk. Research may be required to document the IT practices adopted by public hospitals during the IT post implementation period.

Research also shows that IT risk exists because internal processes, people and systems are controlled inadequately (Kimwele, 2013; Asangansi, 2013; KACCA, 2008; Deloitte, 2012; Taub, 2002; Munene, 2009 and Waema, 2010). This makes one to ask the question: To what extent is this observation true for public hospitals in Kenya?

The study sought to answer the following research question: What is the relationship between IT post implementation practices among public hospitals in Kenya and IT operational risk minimization? This study endeavored to establish the relationship between IT post implementation practices and IT operational risk minimization among the public hospitals in Kenya.

1.3 Research Objectives

The study's main objective was to establish the relationship between IT post implementation practices and IT operational risks minimization in public hospitals in Kenya. The specific objectives are:-

i. To establish the IT post implementation practices in public hospitals in Kenya

ii. To identify the existing IT operational risks in public hospitals in Kenya

iii. To determine the relationship between IT post implementation practices and IT operational risks minimization among public hospitals in Kenya.

1.4 Importance of the Study

The study results should inform the public hospitals of the IT operational risks most of them are exposed to and the relationship between the risks and the IT post implementation practices adopted by them. It is hoped that the hospitals will use this information as a guide in restructuring their organizations for the purpose of better managing IT operational risk with a view to minimizing IT operational risk.

It is hoped that the research findings will assist the government in stipulating policy actions necessary to spur the implementation of IT in the sector. More importantly the government should use the results to evaluate the likelihood of success of it's drive to create functioning IT systems in the public hospitals across the county with the aim of establishing a national health database.

This study seeks to contribute to the literature by broadening the understanding of the IT post implementation practices adopted and the IT operational risks experienced by public hospitals in Kenya. The results could be important in understanding, improving or even developing theories relating to IT post implementation practices.

It is also hoped that IT professionals was learn from the findings and improve on the IT implementation process they used by selecting and improving on the best implementation models. The study also aims to inform IT professionals what happens long after they have handed over the project to a client.

CHAPTER TWO: LITERATURE REVIEW

2.1 Introduction

This chapter discusses the literature related to IT post implementation practices and IT operational risk. The review is conceptualized under the objectives of the study and mainly focuses on Risks in organizations, Information Technology post implementation practices, Information technology operational risks, Post implementation practices and IT operational risk minimization, Theoretical perspectives on IT operational risk, Summary of literature review and The conceptual framework.

2.2 Risks in Organizations

The meaning of risk is used differently by different audiences. It depends on the context where it is applied to support decision making (Charette, 2010). For example, hospital personnel used risk in a context of quality assurance program while safety professional was used risk in a context to reduce accidents and injuries. However, characteristics of risk remain the same for all definitions. For a risk to exist there must be a potential existence for a loss and the presence of uncertainty to a decision making (Charette, 2010). These two conditions form the basic characteristics which risk is defined.

The early literature on risks (Schumpeter, 1934) discussed risk as a good thing and risk taking was a positive action leading to market innovation. Others hold a different view and take risk as inferring possibility that something may go wrong. The Stanford Encyclopedia of Philosophy (2007) explains that risk is an unwanted event with negative consequences. It covers all aspects of organizational activities and it is included in all management levels.

McNaill et al (2010) defined risk as “any event or action that may adversely affect an organization’s ability to achieve its objectives and execute its strategies”. Therefore, the nature of risk, no matter what the area is, can be defined as the possibility of suffering loss. Risk will generally result into the following consequences: Loss of public

confidence, embarrassment, financial losses, targets missed and claims against the organization.

2.3 Information Technology Post Implementation Practices

The successful implementation of IT projects depends on many factors affecting the project's pre-implementation, implementation and post implementation stages. For this study the post implementation stage is the period after the project is handed over to the client by the vendor. Kimwele et al (2005) suggested that appropriate practices, when adopted on an organization-wide level, was allow a standard approach in addressing IT challenges.

During the post implementation period, organizational practices should comprise four elements identified by Karimi (2006) as: data classification, management controls, operational controls and technical controls. Data classification is the classification of data based on its level of sensitivity and the impact to the organization should that data be disclosed, altered or destroyed without authorization. It could be restricted data, private date or public data. Management controls encompass risk management, security controls, business continuation planning, and error correction; operational controls comprise personnel security, physical security, documentation, awareness and training while technical controls comprise identification and certification of identity, logical access control, audit trail and monitoring. This study was concern itself with whether the four elements are present in the practices adopted by organizations to guide IT implementation during the post implementation stage.

The post-implementation phase of software development life cycle is one of the most important aspects of software engineering (Edwards, 2008). This phase comes after the project implementation phase which has one key activity (installing and releasing the new system in its target environment) after which the system enters the operations and maintenance phase for the remainder of the systems operational life; therefore the post implementation phase is an ongoing process (Baars, 2008).

2.4 Information Technology Operational Risks

All major risks faced by a business firm are referred to as enterprise risks and can be classified according to their nature and include strategic risk, operational risk and financial risk. Strategic risk refers to uncertainty of the firm's goals and objectives. Operational risk may result from the firm's business operations; e.g. from services offered and systems in used. Financial risk refers to uncertainty of loss due to adverse effect of commodity prices, interest rates, foreign exchange rate and value of money (COSO, 2004).

According to COSO (2004) operational risk is a risk that results from the firm's business operations; e.g. from services offered using computer systems that hackers may break into The term "operational risk" has been defined only in the past few years, although this type of risk has been present for years. At first, it was commonly defined as "every type of non-quantifiable risk", or "everything other than credit and market risk". Nowadays, there is a large number of definitions.

Operational risk was defined as the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events (BBA, ISDA, RMA and PwC, 1999). This was the first universally accepted definition of the risk. They clarified that this arises from the potential that inadequate information systems; technology failures, breaches in internal controls, fraud, unforeseen catastrophes, or other operational problems may result in unexpected losses or reputation problems. BCBS (2004) later affirmed this definition but added that the risk includes legal risk, but excludes strategic and reputational risks.

The following operational risk definition is used by Credit Suisse Group (2000), as quoted by IIF and Mckinsey & Company (2011):

> Operational risk is the risk of adverse impact to business as a consequence of conducting it in an improper or inadequate manner and may result from external factors. Operational risk may tangibly manifest itself in the likes of business disruption, control failures, errors, misdeeds or external events, and can be

captured in five major risk categories: Organization, Policy/ Process, Technology, Human, External.

The spread of IT applications has recently brought operational risk into focus. This is because IT applications have brought about new problems for organizations. These problems come in form of IT operational risks which are the concern of this study and are discussed in the next section.

Generally, IT risk is a potential damage to an organization's value. It is a major element of risks caused by systems and technology and includes such threats as business interruption, disaster recovery, business and information security, data backup and protection, business license compliance and social media used (Jammal, 2011). IT risk was once a minor component of operational risk but is emerging as a major hazard for organizations to identify and manage (Savić, 2011).

IT risk is the risk of failure or malfunction of IT applications and infrastructure used to support a company (Kitheka, 2013). It is the failure to respond to these requirements, as well as many other issues such as: human error, internal fraud through software manipulation, external fraud by intruders, obsolesce in applications and machines, reliability issues, mismanagement, and of course the effect of natural disasters (BCBS, 2006).

IT systems are increasingly becoming critical to every aspect of business and as a result a company's operations may be highly dependent on the integrity of its IT systems. Its success therefore would depend, in a great part, on the performance of the information system (Savić, 2011). This dependency exposes the organization to IT risk. Badie (2011) adds that IT applications have become more susceptible to IT risks because of the wide spread usage of computers, the interconnectivity of these computers, and rapid development of Internet applications.

2.5 IT Post Implementation Practices and IT Operational Risk Minimization

IT systems can live long after they have been handed over by the vendor. Their success or failure greatly depends on, among other factors, the post implementation practices adopted by an organization. This implies that post implementation practices adopted by an organization affect the IT risk levels of the organization. A large proportion of IT projects end up failing. Quite often the underlying factors are associated with post IT implementation practices that management adopts. For instance, Ramimi et al (2008) concluded that a large number of health information systems implementations fail due to insufficient organizational harmonization; lack of coordination of operations between the end-users and the system suppliers, lack of sufficient technical support, insufficient user training during implementation and misconceptions. The Committee of Sponsoring Organizations of the Treadway Commission (COSO, 2004) asserts that improved IT practices should enhance the efficiency, effectiveness and assurance of internal control processes.

The practices adopted by an organization may provide an uncertain environment where critical areas of IT system issues such as compliance with laws, regulations and standards are neglected. The neglect could lead to the risk of legal liability claims and distorted reputation of an organization. Makau (2010) (as quoted by Munene, 2009) observes that without proper IT governance, IT systems can lose integrity with serious implications on performance and can also result in breach of client confidentiality. IT risks include breakdowns in IT related internal controls and corporate governance, which can lead to financial losses through frauds, or failure to carry out operations in timely manner (BCBS, 2006). Problems associated with enterprise IT applications implementations become more rampant during the post implementation phase because once users learn their way around the system, they can test the systems limits, setting off shockwaves that can devastate an otherwise successful control environment (Musaji, 2005).

2.6 Theoretical Perspectives on IT Operational Risk

This study is guided by the capability maturity model (CMM) and the governance model which explain and give guidance on how a project should be structured and organized to achieve efficiency and avoid risk. The models are discussed in the next sections.

2.6.1 The Capability Maturity Model

The Capability Maturity Model (CMM) was developed at Carnegie Mellon University in the USA between 1986 and 1993 (Paulk et al, 1993). Maturity was explained by Crawford (2007) as the logical way to improve an organization's services, particularly IT services. A maturity model therefore can be viewed as a set of structured levels that describe how well the behaviors, practices and processes of an organization can reliably and sustainably produce required outcomes (Finkelstein, 1998).

A maturity model is specifically used when evaluating the capability to implement data management strategies and the level at which that company could be at risk from said strategies. The more mature an organization is against this benchmark, the less at risk it is in terms of risks associated with poor data management practices.

Alternative project management models include the Portfolio, Programme and Project Management Maturity Model (P3M3) which breaks down the broad disciplines of project management into a hierarchy of key process areas. Another model is the Organizational Project Management Maturity Model (OPM3) which provides a method for organizations to understand their organizational project management processes and measure their capabilities in preparation for improvement and helps them develop the roadmap to improve performance.

2.6.2 Governance Model

A governance model describes the roles that project participants can take on and the process for decision making within the project. In addition, it describes the ground rules for participation in the project and the processes for communicating and sharing within

the project team and community (Gardler et al, 2013). In other words it is the governance model that prevents a project from descending into chaos.

A governance operating model should organize processes and functions such that the board receives the information it requires to effect good governance and management and the business units can conduct their activities in ways that are coordinated. A strong board and governance structure can help an organization weather critical crisis.

One of the commonly used governance models is the technology governance model. The Information Technology Governance Institute (2003) as quoted by Blackmer et al, 2005)) identifies five IT Governance focus areas as strategic IT alignment, value delivery, risk management, resource management and performance measurement. Best practices were identified for each focus area and included an IT advisory board, establishing a help desk, used of policies and procedures and developing strong and broad staff competencies.

2.7 Empirical Review

Organizations are becoming increasingly reliant on IT to fulfill many of their basic functions (Makumbi et al, 2012). IT comes with serious security threats with serious consequences and therefore it must be well protected. The study concluded that small business owners are unclear as to what steps they should take and therefore have not taken the steps to safeguard their businesses.

Nicolaou (2008) found out that the failure of ERP systems was due to a number of factors: initial justification that drives development, system integration problem, lack of user training and failure to understand how IT applications change business processes. He recommended research examines methods to improve ERP systems implementation.

Wekesa (2012) found out that foreign exchange rate risk management has a positive impact on the profits of airlines in Kenya. He also found out that all the airlines sampled had a foreign currency risk management policy, risk management department and monitored the success of the foreign exchange risk policy monthly.

Kimwele et al (2005) found evidence from their survey to suggest that IT security policies are not widely adopted and the benefits harnessed by Kenyan SMEs. Al-Tamimi (2002) found that banks were mainly facing credit risk which they identified through inspection by branch managers and financial statements analysis methods. Al-Tamimi & Al-Mazrooel (2007) found out that the three most important types of risks encountered by banks are foreign exchange risk followed by credit risk and finally operational risk. Their study brought out operational risk, which IT risk is part of, as important to banks.

Wanyonyi (2011) surveyed the foreign exchange risk management practices in organizations and concluded that foreign exchange risk is an important aspect used by multinationals to ensure a safe and sound management as they are exposed to foreign exchange risk. The recommendations were that the risk management department was very important for multinationals.

The Frost and Sullivan (2011) study reported that key risks from an organizations security perspective include application vulnerabilities, mobile devices, viruses and worm attacks, internal employees, hackers, contractors, cyber terrorism, cloud-based services and organized crime. Forrester (2011) reported that security threats were escalating and constituted a major concern. This study sought to establish if the increase in IT security threats is related to post implementation practices adopted by public hospitals.

2.8 Summary of Literature Review

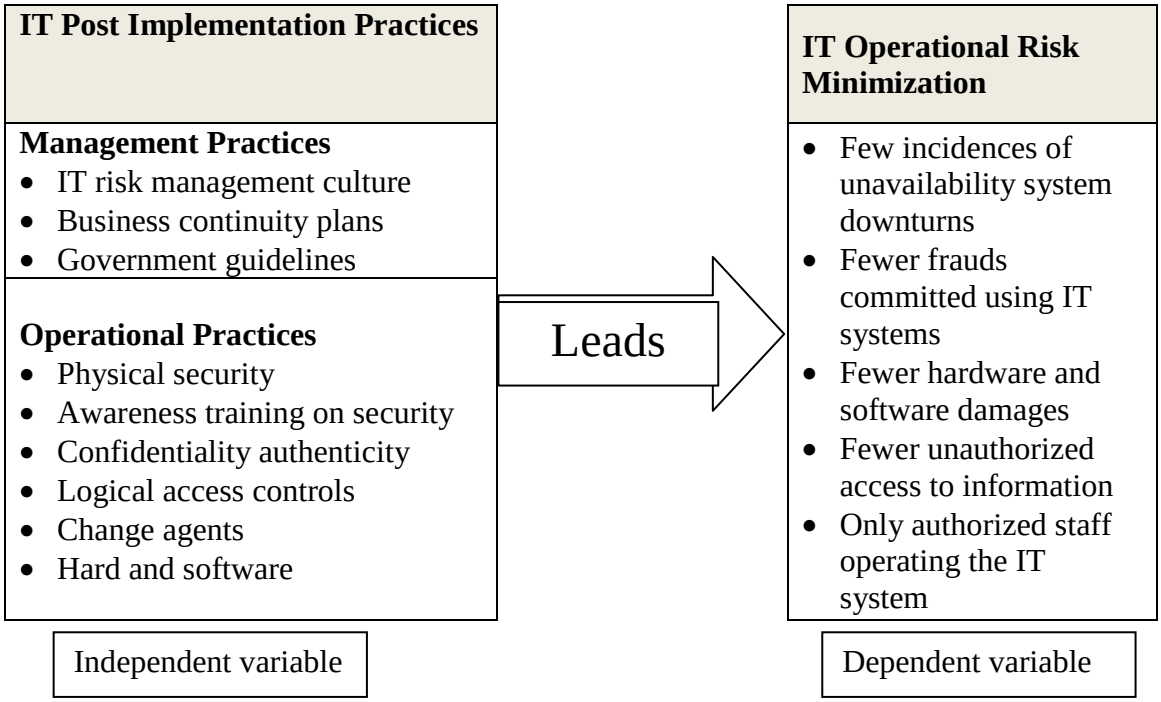
The literature reviewed shows that the studies did not investigate the relationship between post implementation practices and IT operational risk. The researcher therefore finds there is a knowledge gap in literature to warrant a research. This study therefore seeks to fill the existing gap by investigating the relationship between post implementation practices and IT operational risk in public hospitals in Kenya.

2.9 Conceptual Framework

A conceptual framework sets out how the dependent variables are affected through the manipulations in the independent variables. It explains the relationship between the dependent and the independent variables in the study. In this study, the independent

variables are the post implementation practices that are adopted by an organization subsequent to the IT implementation. The dependent variable is IT operational risk. It is considered dependent since this type of risk arises from the failure of systems and technology in an organization due to a wrong practice in the organization or external factors.

Figure 2.1: The Conceptual Model



CHAPTER THREE: RESEARCH METHODOLOGY

3.1 Introduction

This chapter describes the overall methodology that was employed in the study. The following are discussed: research design, study population, research instruments, data validity and reliability, data collection and finally data analysis.

3.2 Research Design

Cooper and Schindler (2008) define research design as the blueprint for the collection, measurement and analysis of data. The study adopted the cross-sectional descriptive research design. Cross-sectional studies are carried out once and represent a snapshot at one point in time (Cooper and Schindler, 2008). The design provides an in-depth account of events, relationships, experience or processes accruing in that particular instance (Mugenda and Mugenda, 1999). This design was preferred because it offered the researcher the opportunity to collect data across several public hospitals at one point in time.

This design was adopted since it provided an opportunity for in-depth study into the IT post implementation practices and IT operational risks in public hospitals in Kenya. It was also adopted as it allowed the researcher to describe the phenomenon as it was, in its environment without any manipulation. It also allowed greater flexibility in terms of time and money as well as the tendency to produce a high response rate. These reasons justified the used of the design in this study.

3.3 Population of the Study

All items of interest in an inquiry constitute a population (Kothari, 2004). The population of the study was all public hospitals in Kenya from Level 3 upwards which have implemented IT systems.

3.4 Sample Design

According to the Ministry Health the only hospitals using ICT systems are these from levels 3 to 6. A master list of hospitals maintained by the Ministry compiled in May 2014 showed that there were 288 public hospitals which fell in this group. Since they are all managed by the Ministry of Health, they have a similar setup, have similar management practices and those of the same level receive the same amount of support from the Ministry. This means that a level 3 hospital in Kiambu has the same characteristics as that of a level 3 in Kakamega. The important thing therefore was to ensure that all levels were represented in the sample.

The public hospitals are spread among the 47 counties in Kenya. Because of time and finances constraints, and given that the public hospitals at the same level have same characteristics the researcher choose to study hospitals that are easily assessable by him and his assistants. The selected counties were Nairobi, Kiambu, Kisii, Embu, Meru and Tharaka Nithi. The sample frame is hereby presented in table 3.1 below:

Table 3.1: The Sample Frame

County	**No. of hospitals**	**Level 3**	**Level 4**	**Level 5/ provincial**	**Level 6**
Nairobi	6	1	1	1	3
Kiambu	9	5	3	1	0
Embu	5	2	2	1	0
Tharaka Nithi	4	1	3	0	0
Meru	14	9	4	1	0
Kisii	15	7	7	1	0
Sample Total	**53**	**25**	**20**	**5**	**3**
National Total	**288**	**135**	**137**	**10**	**6**

Due to the small number of hospitals with IT systems in the counties selected a census survey was used.

3.5 Data Collection

Primary data was collected directly from the hospital administrators and IT system administrators. The data was collected by use of a closed ended questionnaire with separate sections covering each objective. Section one collected bio data of the hospitals and the respondent; section two collected data on objective one (IT post implementation practices); section three collected data on objective two (IT operational risks). The questionnaires were administered by drop and pick method. The questionnaires were delivered by the researcher to the respondents or through well trained and qualified research assistants.

To ensure validity and reliability of the data collection instruments, formulated questionnaires were pre-tested before they are administered to the respondents. The questionnaires were structured to address each of the research objectives. The questionnaire for the pilot test is like a draft that precedes the final report and as Borg and Gall (1989) indicate, the purpose of the pilot exercise was to get problems out of the instrument so that the subject in the researcher's main study would not experience any difficulties in completing the questionnaire.

3.6 Data Analysis

Collected data was coded and analyzed by use of means and standard deviations and presented using tables, graphs and percentages. Objective one and two was analyzed using mean scores with the aid of the Statistical Packages for Social Sciences (SPSS) while objective three was analyzed using multiple regression to find the degree of relationship between the post implementation practices and the IT operational risks. The study used the following regression model to find the relationship between the independent variable and the dependent variable.

$$Y = A+B_1X_1+B_2X_2 + e$$

The predicted (dependent) value of Y is a linear transformation of the X independent (predictor) variables (X1and X2). E is the error. The "B" values are the regression weights.

CHAPTER FOUR: DATA ANALYSIS, FINDINGS AND DISCUSSIONS

4.1 Introduction

This chapter presents the data analysis, findings and discussions in line with the main objective of the study which was to investigate the relationship between the IT post implementation practices and IT operational risk minimization in public hospitals in Kenya. The presentation is in form of tables, figures and narratives. Questionnaires were used to seek the respondents' perceptions of the IT post implementation practices and IT operational risk minimization. Out of the 53 hospitals that were given the questionnaires to fill, only 44 responded and returned the questionnaires; a response rate of 83%.. The data was analyzed with the aid of SPSS. The responses per each of the four hospital categories covered by the study are as presented in table 4.1 below.

Table 4.1: Response rate per hospital level

	Hospital level	Frequency	Percent	Valid Percent
Valid	Level 3	9	20.5	20.5
	Level 4	28	63.6	63.6
	Level 5	4	9.1	9.1
	Level 6	3	6.8	6.8
	Total	**44**	**100.0**	**100.0**

Most of the hospitals in the study are level 4 category hospitals.

4.2 Descriptive Statistics

This section presents the descriptive statistics on the data collected from the respondents.

4.2.1 Years IT System Has Been in Use

Table 4.2 below shows that the length of time the hospitals have been using IT systems varies from one to six years with a mean of 3.36 years. This means that most hospitals have reasonable experience in implementing and operating IT systems.

Table 4.2: Years IT system has been in use

	N	Mean	Std. Deviation
Years of using IT system	44	3.36	1.143

4.2.2 IT Post Implementation Practices

Once an IT system is installed and handed over to the hospital by the vendor the hospital is expected to put in place appropriate practices to facilitate the operation of the system. The IT post implementation practices were categorized and studied under IT post implementation management practices and IT post implementation operational practices. The respondents were asked to respond to questions under each category and the results are summarized in the following sections.

4.2.2.1 IT Post Implementation Management Practices

The respondents were asked to indicate the extent to which they agreed with various statements concerning the IT post implementation management practices adopted by the hospital using a five point likert agree/disagree scale of 1= strongly disagree; 2= disagree; 3= neutral; 4= agree and 5= strongly agree. The results are tabulated in table 4.3 below.

Table 4.3: IT post implementation management practices

IT post implementation management practices	N	Mean	Std. Deviation
Computers are routinely utilized for personal work	44	2.02	1.067
IT risk training is given to staff	44	2.50	1.338
IT tasks are included in job descriptions	44	2.52	1.663
Staff is taught ethical used of IT	44	2.73	1.264
MOH/GOK IT policies & guidelines are adopted	44	2.75	1.465
IT risk is discussed in HMT	44	2.82	1.352
Routine checks for unauthorized SW carried out	44	3.09	1.522
Risk control and management is my responsibility	44	3.18	1.544

According to the findings in table 4.3, the respondents disagree (mean ≤2.99, with a significant standard deviation) that the hospitals allow computers to be routinely utilized

for personal work, IT risk training is given to staff, IT tasks are included in job descriptions, staff members are taught ethical use of IT systems, MOH/GOK policies & guidelines are adopted and that IT risk is discussed in hospital management team meetings (HMTs). The findings too indicate that ((mean ≥3.0≤3.99, with a significant standard deviation) the respondents agreed that routine checks for the use of unauthorized software are carried out and that risk control and management is their responsibility. This indicates that the level of IT risk communication and training is low in the public hospitals that have implemented IT systems in Kenya. It also indicates that IT assets in public hospitals are exposed to a level of IT operational risk.

When the respondents were asked to respond to Yes or No (1 = Yes; 2 = No) questions on IT management practices they responded as tabulated below.

Table 4.4: Questions on IT post implementation management practices

IT post implementation management practices	**N**	**Mean**	Std. Deviation
Are CD drives and USB ports disabled?	44	1.75	0.719
Does an IT risk policy and procedures exist?	44	1.64	0.487
Does the hospital have its own ICT staff?	44	1.80	0.408
Does the hospital have an ICT conversant auditor?	44	1.89	0.321

With a mean of >1.0 the respondents suggest that on average CD drives and USB ports on computers are not disabled, IT risk policies and procedures do not exist, most hospitals do not have their own ICT conversant staff and auditor. The individual responses, on average, were less than 1 point away from the mean. The findings mean that IT systems implementations in the public hospitals are exposed to IT operational risk due to lack of guiding IT policy and procedures and competent ICT staff.

When asked who is responsible for the day-to-day IT matters in the hospital, 55.8% of the respondents indicated that it is the Chief Administrator of the hospital, 18.6% the ICT staff, 7.0% the accountant and 28.65% indicated that other people other than the three are responsible. This is shown in figure 4.1 below. This finding corroborates the finding above that most hospitals lack competent ICT staff of their own. This was further

collaborated when respondents answering to the question 'who manages user rights to the IT system?' responded at 54.5 % that the chief administrator of the hospital is the one who manages and allocates IT system user rights followed by ICT staff at 20.5%, the vendor at 11.4%, the accountant at 4.5% and the users at 9.1%.

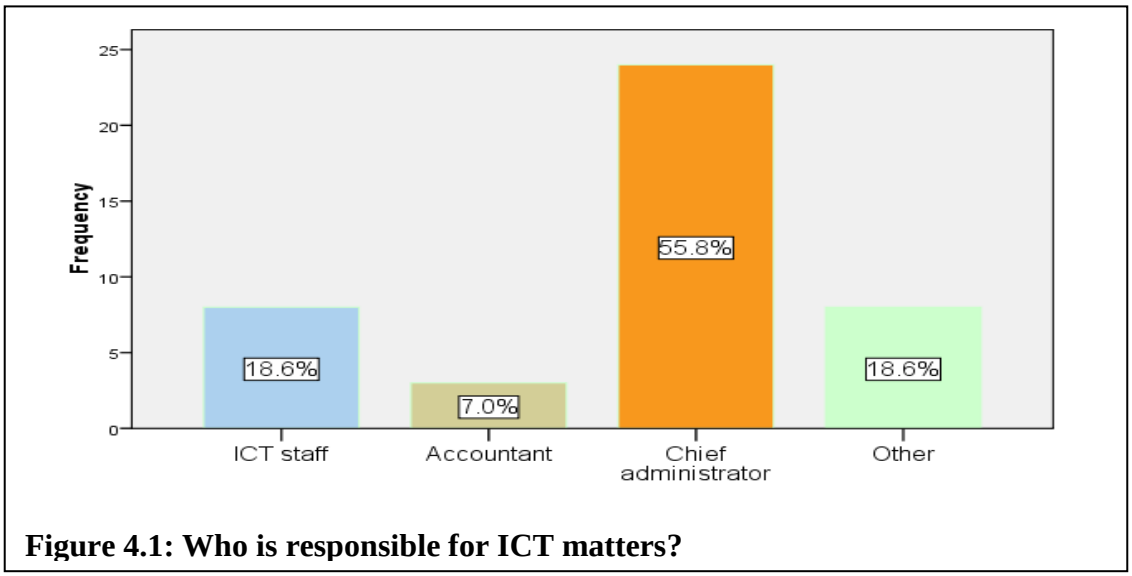


Figure 4.1: Who is responsible for ICT matters?

In response to the question how often is important data backed up, 40.9% of the respondents indicated that it is done on a daily basis, 29.6% on a weekly basis, 22.7% on a monthly basis and 6.8% on intermittent days of the week. This means that most public hospitals are at risk of losing data if IT systems for one reason of the other become unavailable. The finding is shown in figure 4.2 below.

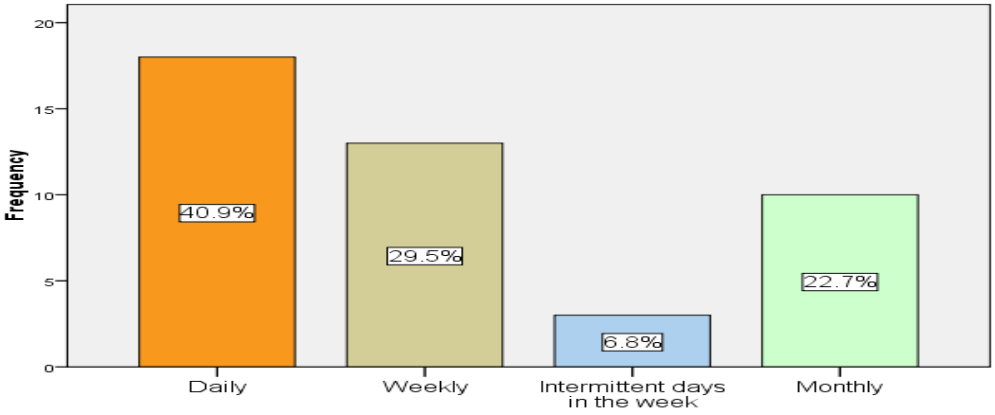


Figure 4.2: How often is important data backed up?

The respondents were asked to indicate the extent to which they agreed with various statements concerning the IT post implementation operational practices adopted by the hospital using a five point likert agree/disagree scale of 1= strongly disagree; 2 = disagree; 3= neutral; 4= agree and 5= strongly agree. These enabled the tabulation and interpretation of the responses from the research instrument. The main statistics derived are mean and standard deviation. The mean illustrated the extent to which the respondents agreed or disagreed with the statements put forth. The results are tabulated in table 4.5 below.

Table 4.5: IT post implementation operational practices

IT post implementation operational practices	N	Mean	Std. Deviation
An IT disaster plan is implemented	44	2.16	1.200
Changes to hardware is documented	44	2.39	1.083
An IT asset use policy is in use	44	2.41	1.282
Hardware movements are formally recorded	44	2.45	1.266
Changes to software are documented	44	2.55	1.302
Staff change their passwords regularly	44	2.59	1.419
Computers are regularly dusted	44	2.68	1.308
Sensitive data and information is encrypted	44	3.02	1.607
Antivirus updated & activated regularly	44	3.09	1.326
Server room is usually locked at all times	44	3.11	1.385
IT maintenance visits are formally authorized	44	3.16	1.430
Database server access is usually restricted	44	3.20	1.488
Users only access software functions they need	44	3.73	1.436
Access to computers is via password	44	3.82	1.263
Staff usually do not share their password	44	4.34	1.180
Software access is usually through password	44	4.41	0.897

According to the findings in table 4.5 above the respondents disagree (mean ≤ 3.50, with a significant standard deviation) that the hospitals staff usually share their passwords, an IT disaster plan is implemented, changes to hardware are documented, an IT asset use

policy exists, hardware movements are formally recorded, changes to software are documented, staff change their passwords regularly, computers are regularly dusted, sensitive data and information is encrypted, antivirus software is updated & activated regularly, the server room is usually locked at all times, IT maintenance visits are formally authorized in writing and database server access is usually restricted.

On the other hand the findings show that the respondents agree (mean ≤3.50≥3.99, with a significant standard deviation) that the users only access software functions that they need to carry on their tasks and that the access to computers hardware is through the use of passwords. The respondents agree (mean ≥4.00, with a significant standard deviation) to a great extent that access to software application is usually through the use of passwords and that staff do not share the passwords. The findings suggest that despite the good management of access rights and passwords, IT systems in public hospitals are greatly exposed to risk arising from the way they are coordinated, operated, secured and changed.

When the respondents were asked to respond to Yes or No (1 = Yes; 2 = No) questions on IT operational practices they responded as tabulated below.

Table 4.6: Questions on IT post implementation operational practices

Question	N	Mean	Std. Deviation
Are unwanted documents shredded?	44	1.77	0.677
Is a risk record kept after a risk incident?	44	1.64	0.613
Is access to server room recorded?	44	1.98	0.340
Is network equipment kept in a lockable place?	44	1.68	0.471
Is there an ICT used policy?	44	1.68	0.561
Is sensitive information lockup?	44	1.45	0.548
Is there an annual IT support agreement?	44	2.00	0.482
Does the hospital have a power generator?	44	1.32	0.471

With a mean ≥ 1.0 the respondents suggest that on average unwanted documents are not shredded or destroyed, a risk record is not kept after a risk incident, the access to server

room is not recorded, the network equipment is not kept in a lockable place, an ICT use policy is not in place, sensitive information is not locked up, no annual maintenance agreement exists between the hospital and the IT system vendors and that most hospitals do not have a power backup or generator. The individual responses, on average, were less than 1 point away from the mean. These findings support the findings in table 4.5 above that IT post implementation operational practices are rudementally and therefore the IT systems are greatly exposed to IT operational risk.

When asked how often virus checks are carried out at the hospital, 52.3% of the respondents said this is only done when a problem occurs, 31.8% said monthly, 9.1% said daily and 6.8% said weekly. This is represented in the figure 4.3 below.

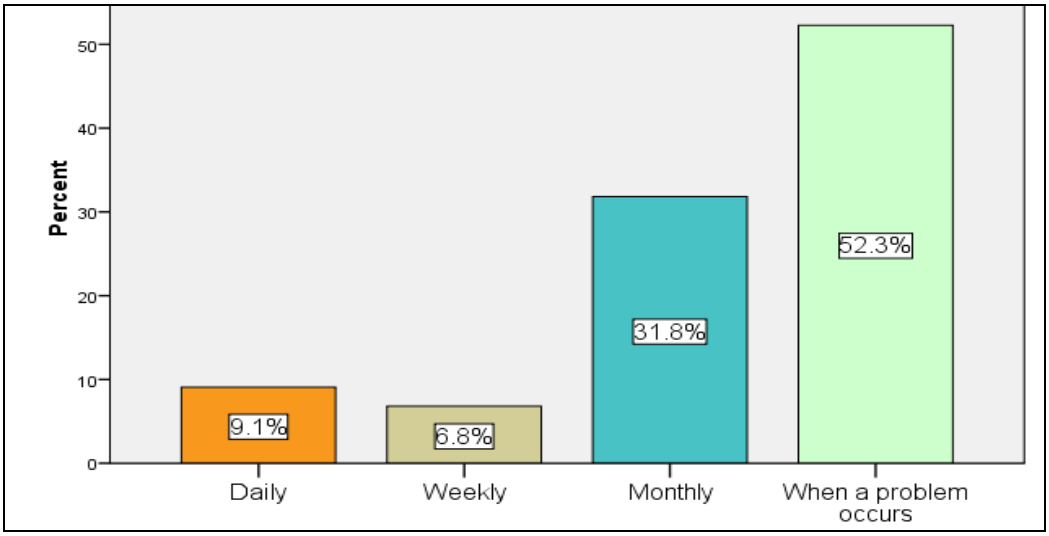


Figure 4.3: How often are virus checks carried out?

When asked how often user passwords are changed, 52.3% of the respondents indicated that user passwords are never changed, 43.2% passwords are changed monthly, 2.3% weekly and 2.3% daily. This is represented in the figure 4.4 below.

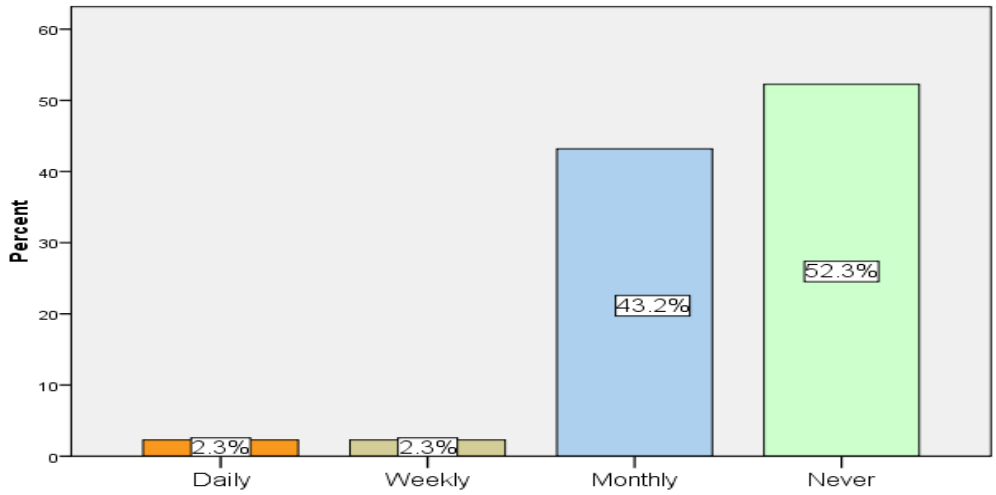


Figure 4.4: How often are user passwords changed?

Figure 4.6 below shows that 43.2% of the respondents indicated that the data server is located in a place easily accessible by the hospital staff, 31.8% in an office of a senior official and 25.0% in a special room.

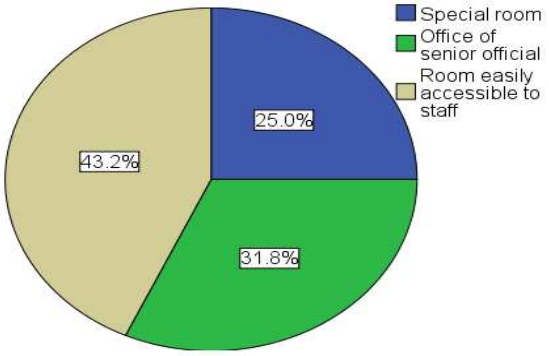


Figure 4.5: Select the office where data server is located

4.2.3 IT Operational Risk Minimization

The respondents were asked to indicate the extent to which they agreed with various statements concerning IT operational risk minimization in the hospital using a five point

likert agree/disagree scale of 1= strongly disagree; 2 = disagree; 3= neutral; 4= agree and 5= strongly agree. The results are tabulated in table 4.7 below.

Table 4.7: IT operational risk minimization

IT operational risk minimization	N	Mean	Std. Deviation
Software breakdowns are minimal	44	2.00	0.747
Interruptions to hospital operations by IT system malfunctioning is minimal	44	2.05	0.861
Hardware breakdowns are minimal	44	2.23	1.008
Staff can operate IT system without vendor's help	44	2.48	1.406
Virus attacks are infrequent or rare	44	2.55	1.170
Fraud arising from internal sources has reduced	44	3.00	1.276
Data backup has helped to restore lost data	44	3.18	1.529
Fraud arising from external sources has reduced	44	3.25	1.332
Few hardware losses occur	44	3.34	1.539
Few unauthorized access incidents witnessed	44	3.57	1.087
Top management supports IT systems	44	3.82	1.084
Loss of cash collected has been minimal	44	4.02	1.023
Vendor support level is adequate	44	4.02	0.976
IT project implementation is going well	44	4.05	0.569

From the findings in table 4.7 above, the respondents disagree (mean $\leq$ 2.99, with a significant standard deviation) that software breakdowns are minimal, interruptions to hospital operations by IT system malfunctioning is minimal, hardware breakdowns are minimal, staff can operate IT system without vendor's help and viruses attacks are infrequent or rare. This means that some part of the IT systems in public hospitals malfunction once in a while and that the hospital staff do not have appropriate skills are experience to IT system problems. This collaborates well with the finding in section 4.2.2.1 that public hospitals lack ICT competent staff.

On the other hand, the respondents agree (mean 3.00 $\leq$ mean $\leq$ 3.99, with a significant standard deviation) that fraud arising from internal sources has reduced due to the

introduction of the IT systems, data backups have helped in restoring lost data, fraud arising from external sources has reduced, few hardware losses occur, few unauthorized access incidents are witnessed and top management supports IT systems. Further the respondents strongly agreed (mean $4.00 \leq$ mean ≤ 5.00, with a significant standard deviation) that loss of cash collected has been minimized.

4.3 Relationship Between IT Post implementation Practices and IT Operational Risk

Linear multiple regression analysis was conducted so as to test the relationship among variables (independent) on IT operational risk. The Statistical Package for Social Sciences (SPSS) was applied to code, enter and compute the measurements of the multiple regressions for the study.

Table 4.8: Model summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	0.794	0.630	0.573	0.47993

R-squared (coefficient of determination) measures how close the data are fitted to the regression line. It explains the extent to which changes in the dependent variable (IT operational risk minimization) can be explained by the change in the independent variables (post implementation IT management practices and post implementation IT operational practices).

The independent variables that were studied explain 63.0% of the IT operational risk minimization as represented by the R square in table 4.8 above. This therefore means that other factors not studied in this research contribute 37.0% to the minimization of the IT operational risk. Further research may be conducted to investigate the other factors not covered by this study.

The significance value of F is 0.002 (Table 4.9) thus the model is statistically significant in predicting IT post implementation practice. The F critical at 5% level of significance is

3.21. Since F calculated (value = 11.072) is greater than the F critical this shows that the overall model is significant.

Table 4.9: Analysis of variance

Model		Sum of Squares	Df	Mean Square	F	Sig.
1	Regression	5.100	2	2.550	11.072	0.002
	Residual	2.994	13	0.230		
	Total	8.095	15			

The multiple regression analysis was conducted so as to determine the relationship between IT operational risk minimization and the two independent variables. Table 4.10 below was generated using SPSS to determine the coefficients of the equation $Y = A+B1X1+B2X2 + \varepsilon$. When the relevant values are extracted from the table the equation becomes:

$Y = 6.075- 0.113\ X1 - 0.811\ X2 + \varepsilon$

Where Y is the dependent variable (IT operational risk minimization), X1 is the IT post implementation management practice and X2 is IT post implementation operational practice.

Table 4.10: Coefficient of determination

Model		Unstandardized Coefficients		Standardized Coefficients		Sig.
		B	Std. Error	Beta	T	
1	(Constant)	6.075	1.144		5.311	0.000
	IT post implementation management practice	-0.113	0.504	-0.047	-0.223	0.827
	IT post implementation operational practice	-0.811	0.223	-0.765	-3.633	0.003

The established regression equation shows that if all independent factors are taken into at constant value zero, IT operational risk minimization will be 6.075. If IT post

implementation management practices is at zero, a unit improvement in IT post implementation operational practices will lead to a decrease of 0.765 in IT operational risk and if IT post implementation operational practices is zero, a unit of IT post implementation management practices will lead to a decrease of 0.047 in IT operational risk. This means that IT post implementation operational practices contributes more to IT operational risk minimization in public hospitals.

At 5% level of significance and 95% level of confidence, IT post implementation operational practices has a p-value of 0.003 level of significance and IT post implementation management practice has p-value of 0.827 level of significant; hence the only significant IT post implementation practice is IT post implementation operational practices.

Table 4.11 below shows the strength of the linear relationship between all the three variables of the study. This relationship is referred to as Pearson's correlation or simply as the correlation coefficient. The relationship between two variables is stronger as the value nears one or minus one. Positive correlation implies an increase of one quantity causes an increase in the other whereas in negative correlation, an increase in one variable will cause a decrease in the other.

The findings in table 4.11 below show that the correlation between IT post implementation management practices and IT operational risk minimization is -0.505. Similarly, the correlation of IT post implementation operational practices and IT operational risk minimization of is -0.793. This means that the relationship between the two independent variables and the dependent variable (IT operational risk minimization) is strong and has a negative direction. If one independent variable changes IT operational risk changes in the opposite direction. The findings also show that IT operational risk minimization is more closely related to IT post implementation operational practices than IT post implementation management practices.

Table 4.11: Pearson's correlation

		IT operational risk minimization	IT Post implementation management practice	IT Post implementation operational practice
Pearson Correlation	IT operational risk minimization	1.000	-0.505	-0.793
	IT Post implementation management practice	-0.505	1.000	0.598
	IT Post implementation operational practice	-0.793	0.598	1.000
Sig. (1-tailed)	IT operational risk minimization	0.000	0.023	0.000
	IT Post implementation management practice	0.023	0.000	0.007
	IT Post implementation operational practice	0.000	0.007	0.000

4.4 Discussion of Findings

This study aimed at establishing the relationship between IT operational risk minimization and IT post implementation practice in public hospitals in Kenya. The findings show that all the hospitals in the study had on average used IT systems for more three or more years and all experience similar IT operational risks. Watangase (2005) while studying the IT environment in banks identified security, data confidentiality, data accuracy, system integration and internal controls as factors influencing IT operational risks. This was supported by MollaZade (2010) who studied factors affecting operational risk of electronic banking and found that data authentication, internal controls, technical infrastructure, access to system and security from the perspective of employees and customers have an effect on operational risk of an organization.

The study found out that the level of training offered to staff on IT security and IT system operations is low and consequently hospitals don't have competent ICT staff to operate

and maintain their IT systems. Mestchian (2005) informs that people risks include employee errors, employee misdeeds, employee unavailability and inadequate employee development and recruitment.

Respondents' opinion is that hospital assets are exposed to a high level of IT operational risk. Related to this they pointed out that data and information backup was not carried out on daily basis. They also indicated that IT policies and procedures were inadequate. These findings were supported by a MOH (2010) health systems assessment report which sited inadequate governance structures and implementation of policy and framework documents and vertical strengthening interventions as some of the major constraining factors hindering the development of hospital information systems in Kenya.

Young (2005) reported that there is an overemphasis on project management leading to the lack of the realization of the importance of the top management support and other issues. The findings show that there is a high support of the top management in the implementation of IT systems in public hospitals. Probably this arises from the fact that the managers are under the watch of the Ministry of Health and that they are on performance contracts.

The findings suggest IT system access rights and passwords are well managed. Sokolov (2008) examined operational e-banking risks in banks and results indicated that security controls and limited unauthorized access to data are the most important factors affecting operational risks. On this score, the public hospitals have done quite well. However the respondents indicated that the passwords are rarely changed thus creating an opportunity for specific security vulnerability or attacks.

Moreover, the findings show that the majority of the hospitals in the study, have no maintenance and support agreements with vendors. However, contrally to expectation in a situation like this, vendor support was found to be adequate. Mestchian (2005) enriches this finding by stressing that technology risks include system failures caused by among others, breakdown and inadequate capacity. The maintenance and support agreements come in handy in minimizing these risks.

External fraud and regulatory changes are some of the external risks caused by actions of external parties (Mestchian, 2005). The respondents indicated that outsiders whose mission in the hospital is to maintain and support it IT systems are not monitored, first, by formally acknowledging their presence through a written document and later documenting any changes or updates to the IT systems. The NEMA/COCIR/JIRA Security and Privacy Committee, in its article *defending medical information systems against malicious software* enriches this study by exposing that vulnerability of an IT system depends on the kind of physical and logical access available to users and on the kind of software running on it. This vulnerability is increased when vendors are allowed access to IT systems without physically monitoring their movements given that as a necessity they may have full logical access rights to the systems.

The beta coefficients for the two IT post implementation practice variables (IT post implementation management practice and IT post implementation operational practice) are -0.047 and -0,765 respectively. This suggests that the IT post implementation operational practice adopted in public hospitals has an inverse relationship with IT operational risk minimization and that IT post implementation operational practice contribute more to IT operational risk minimization than IT post implementation management practice.

The study results are important to public hospitals as they can use them to enrich their IT policies and use them as a guide in restructuring their organizations for the purpose of better managing IT operational risk with a view to minimizing IT operational risk. The Ministry of Health should find the findings useful for the purpose of developing the appropriate long-term IT policies for public hospitals and also for the purpose of supervision. The study adds to the existing literature by the finding that the study independent variables explain 63% of the dependent variable in public hospitals.

CHAPTER FIVE: SUMMARY, CONCLUSIONS AND RECOMMENDATIONS

5.1 Introduction

This chapter presents a summary of the study findings, conclusions and recommendations. It also has a section that the researcher suggests areas for further research.

5.2 Summary of Findings

This study aimed at establishing the relationship between IT post implementation practice and IT operational risk minimization in public hospitals in Kenya. A census survey was conducted for all the public hospitals in the selected six counties of Nairobi, Kiambu, Kisii, Embu, Meru and Tharaka Nithi. A 83% response rate was realized. The data was analyzed with the aid of SPSS.

The first objective of the study was to establish the IT post implementation practice in public hospitals in Kenya. The findings show that the current IT post implementation practice is inadequate. Staff training in IT security and operations is inadequate too, IT policy and procedures do not exist or are inadequate, IT system access rights management practices adequate but are negated by the fact that passwords are rarely changed, no vendor agreements exists, and physical access and movements as well as system changes and updates are not documented.

Objective two sought to identify the existing IT operational risks in public hospitals in Kenya. The findings show that public hospitals experience IT operational risks arising from fraud, unavailable systems due to system breakdowns and lack of backups, and unauthorized access to IT systems due to lack of physical and logical system controls.

The final objective sought to determine the relationship between IT post implementation practice and IT operational risks minimization among public hospitals in Kenya. The findings indicate that there is an inverse relationship between IT Post implementation

practice adopted in public hospitals and IT operational risk minimization. Among the two variables studied IT post implementation operational practice contributes more to IT operational risk minimization than IT post implementation management practice.

5.3 Conclusions

On the basis of objective one, it is concluded that the current IT implementation practice in public hospitals is inadequate for IT operational risk minimization. There lack of hospital-wide policies and procedures describing, among other things, IT system security, use and operation, expectations of users and the sanctions available if they are negligent on the one hand, or willful on the other, in their disregard of them.

On the basis of objective two, it is concluded that IT systems in public hospitals in Kenya are exposed to a high level IT operational risks arising from fraud, unavailable systems due to their breakdowns and lack of data backups, and unauthorized access to IT systems due to lack of physical and logical system controls.

Arising from objective three, it is concluded that there is an inverse relationship between IT post implementation practice adopted in public hospitals and IT operational risk minimization. Among the two IT post implementation practice variables studied, IT post implementation operational practice contributes more to IT operational risk minimization than IT post implementation management practice.

5.4 Recommendations

Based on the findings, it is recommended that the hospitals implement comprehensive policies and procedures to guide IT operations and administrative issues. These should be documented in a manual, explained and made available to all staff. To control the physical access and movement of all users who are not employees of the hospital, it is recommended that any visits in relation working on the IT assets be formally documented in writing, and access to data server and other important data be monitored through the use of registers. By doing so, two very important IT security controls will be achieved –

physical and logical access controls. It is also recommended that staff be regularly trained on IT security matters.

To minimize the risk of unavailable systems, it is recommended that all IT assets that require regular maintenance be under a support agreement. This should elicit quick response from vendors whenever they are needed. It is recommended also that IT system changes and updates be documented. This will mitigate associated risks such as information being corrupted and/or destroyed, computer performance being disrupted and/or degraded, productivity losses being incurred and exposure to reputational risk.

Finally, it is recommended that the hospital management take advantage of the accumulated knowledge on IT systems to provide leadership towards enacting appropriate institutional risk strategy and risk management framework. The management could also infuse risk ownership, control and management responsibilities through job descriptions and performance goals.

5.5 Limitations of the Study

Various challenges were encountered during this study. The study covered only public hospitals in Kenya. This was due to time and other resources. A wider coverage including private and other hospitals could have yielded a more informative result. The response rate was 83% mainly because the respondents were too busy to attend to the questionnaire.

5.6 Suggestions for Further Research

A study is recommended to find the relationship between, IT pre-implementation practice, IT post implementation practice and IT operation risk minimization. This would help public hospitals to have a fuller understanding of all the variables contributing to IT operational risk minimization. A comparative study with the private hospitals aimed at establishing a benchmark for IT post implementation practices is recommended. The study needs to be widened to other sectors of the economy such as insurance, tourism and manufacturing.

REFERENCES

Al-Tamimi, H. (2002). *Risk management practices - An empirical analysis of the UAE commercial banks*. United Arab Emirates.

Akbari, P., Rezavandi, R., Vatandost, T., & Baharestan, O. (2012). A study on factors affecting operational electronic banking risks in Iran banking industry case study: Kermanshah Melli Bank of Kermanshah. *Journal of Applied and Basic Sciences*.

Asangansi, I. (2012). Understanding HMIS implementation in a developing country ministry of health context - An institutional logics perspective. *Journal of Public Health Informatics*. Published online Dec 19, 2012.

Baars ,W. (2008). *Project lifecycle phases, project management best practices*.

Badie, F. (2011). *International Journal of Technology, Knowledge & Society, 7*(1), 13. Michigan, USA.

Basel Committee on Banking and Supervision. (2006). *International convergence of capital measurement and capital standards: A revised framework.*

Basel Committee on Banking and Supervision. (2004). *Sound practices for the management and supervision of operational risk.*

BITS Financial Services Roundtable. (2004). *BITS key risk measurement tool for information security operational risks.*

Blackmer, G., Kahn, D., Fercak, A., & Meross, S. (2005). *Best practices for information technology governance. City of Portland audit report*. Oregon: City of Portland.

Bogue, R. L. (2005). Four steps for reducing project risk. Retrieved from http://www.techrepublic.com /article/four-steps-for-reducing-project-risk/

British Bankers' Association, International Swaps and Derivatives Association and Association, Risk Management Association, & PricewaterhouseCoopers. (1999). *Operational risk, the next frontier*. Philadelphia: RMA.

Charette, R. N. (1991). *Applications strategies for risk analysis.* Texas: Mcgraw Hill.

Cooper, D. R. & Schindler, P. S. (2008). *Business research methods*. New York: McGraw-Hill Higher Educated.

COSO. (2004). *Enterprise Risk Management—Integrated framework executive summary*.

Crawford, J. K. (2007). *Project management model (*2nd ed*).* New York: Auerbach Publications.

Deloitte East Africa. (2012). *Enterprise risk management survey report 2012*. Deloitte East Africa.

Edwards, H. K. (2008). *Post-implementation management in large-scale management information systems: Changes, incident reports, help desk calls, and business process.* University of Hawaii, U.S.A.

Ernst & Young. (2011). *Global information security survey.* Ernst & Young

Finkelstein. A. K. J., (1998). *A software process immaturity model*. London: John Wiley & Sons.

Forrester Consulting. (2011). *The total economic impact of IBM's Netezza data warehoused appliance with advanced analytics*.

Frost, J., & Sullivan, B. (2010). *The 2011 global information security workforce study*. Retrivied from https //www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content /GISWS/CXO-and-Security-Executive-Brief-ISC2-frost.pdf

Gardler, R., & Hanganu, G. (2010). *Governance Models.* Retrieved from http://oss-watch.ac.uk/resources/governancemodels

Gladwin, J., Dixon, R. A., & Wilson, T. D. (2003). *Implementing a new health management information system in Uganda*. United Kingdom: University Press.

Gray, C, & Larson, E. (2008). *Project management – the managerial* process (4th ed). New York: McGraw Hill.

Hornstein, H. (2008). Using a change management approach to implement IT programs. *Ivey Business Journal.*

Hughes, G. (2006). *Five steps to IT risk management best practices*.

IIF & Mckinsey & Company. (2011). *Risk IT and operations: Strengthening capabilities.*

Jammal, M. I. F. (2011). Information technology at the forefront of operational risk: Banks are at a greater risk. *Journal of Operational Risk*. Published online.

Karimi, Z. (2006). *To provide a conceptual model for evaluating information security risks:* Case study: Sepah Bank of Iran.

Kenya Anti-Corruption Commission Authority (KACCA). (2008). *Corruption prevention guidelines on ICT systems in the public sector, directorate of prevention services*.

Kimama, F. M. (2011). *Challenges facing the implementation of hospital management information systems in hospitals in Nairobi*. Retrieved from erepository.uonbi.ac.ke/

Kimwele, M. W. (2013). *Information technology (IT) security in small and medium enterprises (SMEs).* Berlin: Springer Berlin Heidelberg.

Kimwele, M., Mwangi. W., & Kimani, S. (2005). Adoption of information technology security policies: case study of Kenyan small and medium enterprises (SMEs). Journal of Theoretical and Applied Information Technology.

Kitheka, P. M. (2013). *Information security management systems in public universities in Kenya: A gap analysis between common Practices and industry best practices.* (Unpublished MBA project, University of Nairobi, Nairobi).

Kothari, C. R. (2004). *Research methodology: methods & techniques*. New Delhi: New Age International Publishers.

Makumbi, L., Miriti, E. K., & Kahonge, A. M. (2012). An Analysis of information technology (IT) security practices: A case study of Kenyan small and medium enterprises (SMEs) in the financial sector. *International Journal of Computer Applications, volume 57, No.18*, November 2012.

McNaill, A. J., Frey, R., & Embrechts, P. (2010). Quantitative risk management-concepts, techniques and tools. New Jersey: Princeton University Press.

Ministry of Health. (2010). Kenya health assessment system. Nairobi: United States Agency for International Development.

MollaZade. (2010). Study of Effective Factors at the E-banking Operational Risk in the Maskan Bank. The Master of Business Administration, Islamic Azad University, Kermanshah Branch, Iran.

Mugenda, O. & Mugenda, A. (1999). *Research methods: Quantitative and qualitative approaches.* Nairobi: Acts Press.

Munene, J. K. (2009). IT governance practices in commercial banks in Kenya (unpublished MBA project, University of Nairobi, Kenya).

Murphy, C. 2010. Reducing risk and increasing probability of success: IT software development just isn't working. London: Liemur Limited.

Musaji, Y. (2005). ERP post implementation problems. Information Systems Audit and Control Association. *Journal Online*. Retrieved from www.isaca.org.

Nicolaou, A. I. (2008). *ERP systems implementation: drivers of post-implementation success.* Bowling Green State University, Ohio, USA.

Önal, M. Z. (2007). *An aggregated information technology checklist for operational risk management.*

Paulk, M. C., Curtis, B., Chrissis, M. B., & Weber, C. V. (1993). *Capability maturity model for software version 1.1*. Carnegie Mellon University, Pennsylvania, USA.

Ramimi, B., Moberg, A., Timpka, T., & Vimarlund, V. (2008). *Implementing an integrated computerized patient record system: Towards an evidence-based information system implementation practice in healthcare.* Retrieved from http:// www.ncbi.nlm.nih.gov/pmc/articles/PMC2655989/

Savić, A. (2011). *Managing IT-related operational risks*. Belgrade: ICT College.

Schumpeter, J. A. (1934). *The theory of economic development.* New York: Harvard University Press.

Shevchenko, P. V. (2010). *Modeling operational risk using bayesian inference*. New York: Springer Heidelberg Dordrecht.

Sokolov, D. (2008). E-Banking: Risk Management Practices of Estonian Banks. TUTWPE, No 156 PP l-34. Available at:http://ideas.repec.org/p/ttu/wpaper/ 156.html.pdf.

Straub, D. W., & Welke, J. (1998). *Coping with systems risk: Security planning models for management decision making.*

Taub, S. (2002). *More corporate crimes and misdemeanors.* Retrieved from www.cfo.com

The Stanford Encyclopedia of Philosophy. (2007). Retrieved from http://plato. stanford.edu/ entries/risk/

Thuku, M. K. (2012). *Relationship between risk management practices and organizational performance of universities in Kenya* (Unpublished MBA project, University of Nairobi, Kenya).

Waema, T. M., & Ndung'u, M. N. (2012). *Understanding what is happening in ICT in Kenya analysis of the ICT sector - A supply- and demand side*. Nairobi: University of Nairobi.

Waema, T. M., Adeya, C., & Ndung'u, M. N. (2010). *Towards Evidence-based ICT policy and regulation.* Nairobi: University of Nairobi.

Wanyonyi, S. K. (2011). *Survey on the foreign exchange risk management practices of Kenyan based subsidiaries of multinational corporations.* (Unpublished MBA Project, University of Nairobi, Kenya.

Watangase, T. (2005). Supervisory in an It Environment. Bus Review, No 75, Available:http//:www.bis.org/review/r.50519c.pdf.

Wekesa, M. S. (2012). *The relationship between foreign exchange risk management and* profitability of airlines in Kenya (Unpublished MBA project, University of Nairobi).

Woods, M. (2009). A contingency theory perspective on the risk management control system within Birmingham City Council. Management Accounting Research, 20.

APPENDICES

APPENDIX I: QUESTIONNAIRE

This questionnaire seeks your responses on IT post implementation practices adopted by your hospital and information technology (IT) operational risk minimization in the hospital.

SECTION A: General Information (Please tick as appropriate).

1. Name of the Hospital_____
2. Classify level of the hospital
   ( ) Level 6
   ( ) Level 5
   ( ) Level 4
   ( ) Level 3
3. Approximately how many years has the hospital been using the IT systems?
   .....
4. Name of the information technology system in used……

SECTION B: Information Technology Post Implementation Practices

5. Kindly indicate the extent to which you agree with the following statements concerning current IT post implementation practices in managing the information technology systems in the Hospital.

Used the scale of:

1= Strongly disagree; 2 = Disagree; 3 = Neutral; 4= Agree and 5= Strongly agree

IT post implementation management practices	**Strongly disagree**	**Disagree**	**Neutral**	**Agree**	**Strongly agree**
IT risk training given to staff is adequate					
Staff adequately taught ethical used of IT					

IT tasks sufficiently included in job descriptions					
Computers routinely utilized for personal work					
MOH/GOK IT guidelines adopted					
IT risk is sufficiently discussed in HMT					
Routine checks for unauthorized SW carried out					
ICT assets are exposed to risk					
Risk control and management is my responsibility					
IT risk training given to staff is adequate					

6. Are CD drives and USB ports in computers used by cashiers, billing clerks, doctors and other system users disabled?

   ( ) Yes ( ) No

7. Does the hospital have a risk management policy and procedure?

   ( ) Yes ( ) No

8. Does the hospital have staff specifically employed to perform ICT duties?

   ( ) Yes ( ) No

9. Who is ultimately responsible for the day-to-day ICT matters in the hospital?

   ( ) ICT staff

   ( ) Accountant

   ( ) Chief Administrator

   ( ) Other

10. How often is important electronic data and information backed-up (tick as appropriate)

    ( ) Daily

    ( ) Weekly

    ( ) Intermittent days in a week

    ( ) Monthly

11. Does the hospital have an internal Information Technology conversant auditor?

    ( ) Yes ( ) No

12. Kindly indicate the extent to which you agree with the following statements concerning existing information technology post implementation operational practices in place at your Hospital.

Used the scale of:

1= Strongly disagree; 2 = Disagree; 3 = Neutral; 4= Agree and 5= Strongly agree

IT post implementation operational practices	**Strongly disagree**	**Disagree**	**Neutral**	**Agree**	**Strongly agree**
Changes to SW are documented					
Changes to HW are documented					
An IT disaster plan is implemented					
An IT asset used policy is in used					
Server room is usually locked at all times					
DB server access is usually restricted					
Computers are regularly dusted					
HW movements are formally recorded					
IT maintenance visits are formally authorized					
Access to computers is via PW					
SW access is usually through PW					
Staff usually share their PW					
Staff change their PW regularly					
Sensitive data and information is encrypted					
Users only access SW functions they need					
Antivirus updated & activated regularly					

13. Are unwanted documents shredded or destroyed?

    ( ) Yes ( ) No

14. Is a risk record kept after a risk incident?

    ( ) Yes ( ) No

15. Please Select the office where data server is located

    ( ) In its own special room

    ( ) In the office of a senior official

    ( ) In an room where it is used by staff or staff can easily access it

16. Is there a system (biometric registration, record book) to identify and record those who enter the server room?

    ( ) Yes ( ) No

17. Are the main switches, routers supporting the IT network in a lockable place?

    ( ) Yes ( ) No

18. Is there an ICT used policy covering for instance – who should keep the server keys, disciplinary process for dealing with unethical behavior, used of unauthorized software in hospital computers, storage of backups etc

    ( ) Yes ( ) No

19. Are devices that contain sensitive information looked up in a safe place?

    ( ) Yes ( ) No

20. How often are the computers checked for viruses?

    ( ) Daily ( ) Weekly ( ) Monthly ( ) When a problem occurs

21. How often are user passwords changed?

    ( ) Daily ( ) Weekly ( ) Monthly ( ) Never

22. Who manages and allocates access rights to the users?

    ( ) ICT staff in charge of ICT function

    ( ) Chief administrator of the hospital

    ( ) The accountant

    ( ) Users

    ( ) Vendor of the systems

23. Is there an annual IT support agreement for the IT systems with the vendors?

    ( ) Yes ( ) No

24. Does the hospital have a power backup or generator

    ( ) Yes ( ) No

SECTION C: IT operational risk minimization

25. Kindly indicate the extent to which you agree with the following statements concerning information technology operational risk minimization in the hospital.

Used the scale of:

(1) Strongly disagree (2) Disagree (3) Neutral (4) Agree (5) Strongly agree

IT operational risk minimization	Strongly disagree	Disagree	Neutral	Agree	Strongly agree
Fraud arising from internal sources has reduced					
Fraud arising from external sources has reduced					
Staff can operate IT system without vendor's help					
HW breakdowns sometimes are experienced					
SW breakdowns are sometimes experienced					
Loss of cash collected has been minimal					
Hardware losses occur					
IT systems are attacked by viruses frequently					
Few unauthorized access incidents witnessed					
Data backup has helped to restore lost data					
Top management supports IT systems					
Vendor support level is adequate					
Sometimes operations are interrupted by IT malfunction					
Fraud arising from internal sources has reduced					

APPENDIX II: LIST OF PUBLIC HOSPITALS IN THE STUDY

	Facility Name	County	Facility Type
1	Kianjokoma Sub-District Hospital	Embu	Level 3
2	Mbeere District Hospital	Embu	Level 2
3	Ishiara Sub-District Hospital	Embu	Level 3
4	Runyenjes District Hospital	Embu	Level 4
5	Embu Provincial General Hospital	Embu	Level 5
6	Thika Level 5 hospital	Embu	Level 5
7	Gatundu District Hospital	Kiambu	Level 4
8	Kihara Sub-District Hospital	Kiambu	Level 3
9	Kirwara Sub District	Kiambu	Level 3
10	Kiambu District Hospital	Kiambu	Level 4
11	Igegania Sub-District Hospital	Kiambu	Level 3
12	Nyathuna Sub District Hospital	Kiambu	Level 3
13	Ruiru Sub-District Hospital	Kiambu	Level 3
14	Tigoni District Hospital	Kiambu	Level 4
15	Kenyenya District Hospital	Kisii	Level 4
16	Keumbu Sub-District Hospital	Kisii	Level 3
17	Masimba Sub-District Hospital	Kisii	Level 3
18	Marani District Hospital	Kisii	Level 4
19	Kisii Hospital (Level 5)	Kisii	Level 5
20	Ibacho Sub-District Hospital	Kisii	Level 3
21	Ibeno Sub-District Hospital	Kisii	Level 3
22	Iyabe District Hospital	Kisii	Level 4
23	Gucha District Hospital	Kisii	Level 4
24	Etago Sub-District Hospital	Kisii	Level 3
25	Gesusu Sub-District Hospital	Kisii	Level 3
26	Nduru District Hospital	Kisii	Level 4

27	Nyacheki Sub-District Hospital	Kisii	Level 3
28	Nyamache District Hospital	Kisii	Level 4
29	Miathene District Hospital	Meru	Level 4
30	Mikinduri Sub-District Hospital	Meru	Level 3
31	Mikumbune Sub-District Hospital	Meru	Level 3
32	Mbeu Sub-District Hospital	Meru	Level 3
33	Meru District Hospital	Meru	Level 5
34	Kinoro Sub-District Hospital	Meru	Level 3
35	Kibirichia Sub-District Hospital	Meru	Level 3
36	Kanyakine District Hospital	Meru	Level 4
37	Githongo District Hospital	Meru	Level 4
38	Giaki Sub-District Hospital	Meru	Level 3
39	Muthara Sub-District Hospital	Meru	Level 3
40	Mutuati Sub-District Hospital	Meru	Level 3
41	Nyambene District Hospital	Meru	Level 4
42	Timau Sub-District Hospital	Meru	Level 3
43	Kenyatta National Hospital	Nairobi	Level 6
44	Spinal Injury Hospital	Nairobi	Level 6
45	Mbagathi District Hospital	Nairobi	Level 4
46	Mathari Hospital	Nairobi	Level 6
47	Dagoreti Sub District Hospital	Nairobi	Level 3
48	Pumwani Maternity Hospital	Nairobi	Level 5
49	Mama Lucy Kibaki Hospital	Nairobi	Level 5
50	Magutuni District Hospital	Tharaka Nithi	Level 4
51	Kibunga Sub-District Hospital	Tharaka Nithi	Level 3
52	Chuka District Hospital	Tharaka Nithi	Level 4
53	Tharaka District Hospital	Tharaka Nithi	Level 4