INFORMATION TECHNOLOGY RISK MANAGEMENT AS A STRATEGIC ENABLER IN TAX REVENUE ADMINISTRATION: THE KENYAN CONTEXT

BY

MUCHIRI CHARLES MWANGI

A Research Project Report Submitted to the Chandaria School of Business in Partial Fulfillment of the Requirement for the Degree of Masters in Business Administration

UNITED STATES INTERNATIONAL UNIVERSITY - AFRICA

SPRING 2015
STUDENT’S DECLARATION

I, the undersigned, declare that this is my original work and has not been submitted to any other college, institution or university other than the United States International University Africa for academic credit.

Signed: __________________________ Date: ________________________________

Muchiri Charles Mwangi (ID 626961)

This research project has been presented for examination with my approval as the appointed supervisor.

Signed: __________________________ Date: ________________________________

Dr. Paul Katuse

Signed: __________________________ Date: ________________________________

Dean, Chandaria School of Business
COPYRIGHT

This work is the product of the author, hence no part of this paper shall reproduced or transmitted electronically, or mechanically including photocopying, reprinted or redesigned without the prior permission of the author.

© 2015 by Charles Mwangi Muchiri.
ABSTRACT

The purpose of this study was to examine a detailed framework for the management of information technology risks in tax revenue administration for strategic agility using Kenya as a context of Less Developed Countries (LDCs). It was led by the following questions; what is the nature of information technology risks?, what are components of IT risk management and what processes are involved?, what are the challenges in IT risk management in the tax revenue administration Kenyan context? And how can enterprises formulate enterprise risk management framework to enable the desired strategic agility?

Descriptive research design method was used in this study. The target population size of this study was 288 Kenyan Revenue Authority management officials, specifically Information Technology and business executives of the revenue authority. The acceptable margin of error used in this study was 5% while the required confidence level was 95% for this study. A sample size of 44 was chosen from this population set for the purpose of surveying through questionnaires. A stratified sample was used to ensure maximum representation of all management staff who in one way or another get involved in the IT risk management process.

Quantitative methods were used to report on the descriptive statistics; these included analyses of the data in terms of frequencies and measures of central tendency through mean and mode. Qualitative data was summarized and categorized according to common themes and presented in frequency distribution tables. Conclusions and recommendations of the report were based on qualitative data and the research objectives were clearly defined; hence, the descriptive research was used to obtain summary measures to address the research questions.

The finding of the study revealed that majority of the respondents were able to identify components of IT risks and also felt that it was fairly developed and that an effective framework would improve performance through more robust corporate planning, effectiveness in achieving organization’s objectives, improved quality of service delivery to taxpayers and consumers. It was also revealed that an effective risk management framework would lead to increased recognition and uptake of opportunities.
A major conclusion from the study findings was that one of the greatest challenges in identifying and assessing risks in tax administration information systems is the complexity of the Kenya Revenue Authority as an organization. In addition, it was concluded that an effective IT risk management capability is an important metric in understanding how IT enables or constrains business initiatives. From the research study, it was recommended that appropriate tools specifically tailored to suit the organization's environment should be developed to harmonize and facilitate identification, classification and documenting of risks. The study also recommended that analytical tools that better capture risk characteristics should be used.

This study will be of great importance to other researchers and academicians who seek to understand how organizations can gain strategic agility through effective management of information technology risks in their organizations, especially in tax revenue administration Kenya as a context of developing countries.
ACKNOWLEDGEMENT

I take this opportunity to sincerely thank my supervisor for his academic guidance and support throughout my research. I would also like to thank my family and specially my wife who have been of great moral support in seeing me through my project.
# TABLE OF CONTENTS

- **STUDENT’S DECLARATION** ................................................................. ii
- **COPYRIGHT** .................................................................................. iii
- **ABSTRACT** .................................................................................... iv
- **ACKNOWLEDGEMENT** .................................................................. vi
- **TABLE OF CONTENTS** ................................................................. vii
- **LIST OF TABLES AND FIGURES** ................................................. x
- **CHAPTER ONE** .............................................................................. 1
  - 1.0 INTRODUCTION ........................................................................... 1
    - 1.1 Background of the Study ......................................................... 1
    - 1.2 Statement of the Problem ...................................................... 3
    - 1.3 Purpose of the Study ............................................................... 5
    - 1.4 Research Questions ................................................................. 5
    - 1.5 Importance of the Study ......................................................... 5
    - 1.6 Scope of the Study ................................................................. 6
    - 1.7 Definition of Terms ................................................................. 6
    - 1.8 Chapter Summary ................................................................. 7
- **CHAPTER TWO** ............................................................................. 8
  - 2.0 LITERATURE REVIEW ............................................................. 8
    - 2.1 Introduction ............................................................................ 8
    - 2.2 Nature of Information Technology Risks ............................... 8
    - 2.3 Components of Information Technology Risk Management .... 13
    - 2.4 Challenges in IT Risk Management ...................................... 19
  - 2.5 Technology Risk Management Formulation for strategic agility .. 23
    - 2.6 Chapter Summary ................................................................. 26
- **CHAPTER THREE** ....................................................................... 27
3.0 METHODOLOGY .................................................................................................................. 27
  3.1 Introduction .......................................................................................................................... 27
  3.2 Research Design .................................................................................................................. 27
  3.3 Population and Sampling Design ....................................................................................... 28
  3.4 Data Collection Methods .................................................................................................... 30
  3.5 Research Procedures .......................................................................................................... 30
  3.6 Data Analysis and Presentation .......................................................................................... 30
  3.7 Chapter Summary ............................................................................................................... 31

CHAPTER FOUR .................................................................................................................. 32
4.0 RESULTS AND FINDINGS ................................................................................................. 32
  4.1 Introduction .......................................................................................................................... 32
  4.2 The nature of information technology risks ....................................................................... 33
  4.3 components of IT risk management and the processes involved ....................................... 35
  4.4 Challenges In Technology Risk Management .................................................................. 40
  4.5 Effectiveness of Enterprise IT Risk Management .............................................................. 41
  4.6 Chapter Summary ............................................................................................................... 48

CHAPTER FIVE .................................................................................................................. 50
5.0 DISCUSSION, CONCLUSIONS AND RECOMMENDATIONS ...................................... 50
  5.1 Introduction .......................................................................................................................... 50
  5.2 Summary .............................................................................................................................. 50
  5.3 Discussion ............................................................................................................................ 52
  5.4 Conclusion ............................................................................................................................ 57
  5.5 Recommendations ............................................................................................................. 59
    5.5.1 Recommendations for Improvement ......................................................................... 59
    5.5.2 Recommendations for Further Studies ..................................................................... 60
LIST OF TABLES AND FIGURES

TABLES

Table 1: Table for determining sample size from the given population size ................................................................. 29
Table 2: Table showing sample size and the respondents interviewed ................................................................. 32
Table 3: Respondent’s Length of Service ................................................................................................................. 33
Table 4 Showing strategic risks .......................................................................................................................... 34
Table 5 Showing operational risks ...................................................................................................................... 35
Table 6 Components of IT risks .......................................................................................................................... 36
Table 7: IT risks Responsibility .......................................................................................................................... 36
Table 8: Presences of the risk register .................................................................................................................. 37
Table 9: The risk register details .......................................................................................................................... 38
Table 10: Tools and techniques for identifying risks .............................................................................................. 39
Table 11: Challenges in risk management ........................................................................................................... 40
Table 12: Partner impediments in developing risk management plans ...................................................................... 41
Table 13: Organization review of risk profile ......................................................................................................... 42
Table 14: Extent/scope and responsibilities for risk analysis .................................................................................. 43
Table 15: Analysis of risk difficulty ....................................................................................................................... 44
Table 16: Risk level for last 5 years ......................................................................................................................... 44
Table 17: Key indicators to monitor organizational risks ........................................................................................ 45
Table 18: Is Risk management process subject to audits .......................................................................................... 46
Table 19: Risk management subject to internal improved performance .................................................................. 46
Table 20: Overall level of risk management practice development ............................................................................ 47
FIGURES

Figure 1: Enterprise IT Risk Framework ................................................................. 15
Figure 2: Risk Profile for GCI .............................................................................. 16
Figure 3: Showing percentage of respondents length of service................................. 33
Figure 4: Showing strategic risks ........................................................................... 34
Figure 5: Showing operational risks ......................................................................... 35
Figure 6: Components of IT risks ........................................................................... 36
Figure 7: IT risks Responsibility ............................................................................. 37
Figure 8: Presence of the risk register ..................................................................... 37
Figure 9: The risk register details ............................................................................ 38
Figure 10: Tools and techniques for identifying risks ................................................ 39
Figure 11: Challenges in risk management ............................................................ 40
Figure 12: Partner impediments in developing risk management plans ..................... 41
Figure 13: Organization review of risk profile ......................................................... 42
Figure 14: Extent/scope and responsibilities for risk analysis ..................................... 43
Figure 15: Analysis of risk difficulty ....................................................................... 44
Figure 16: Risk level for last 5 years ...................................................................... 45
Figure 17: Key indicators to monitor organizational risks .......................................... 45
Figure 18: Is Risk management process subject to audits ........................................ 46
Figure 19: Risk management subject to internal improved performance ................... 47
Figure 20: Overall level of risk management practice development .......................... 47
CHAPTER ONE

1.0 INTRODUCTION

1.1 Background of the Study

Every enterprise faces a large number of risks as part of doing business. Problem solving and decision making, be they technological or business-related in nature, are performed in environments of varying degrees of uncertainty (Zeid, 2014). The uncertainty is, however, not wholly exogenous, but relative to the problem-solving capability. Strategy as a formal discipline has its origins in the planning of warfare. The very term strategy is derived from the Greek word *strategos*, meaning a military leader, commanding both sea and land operations. Strategy is the science and art of planning for battle, as opposed to tactics, which involve methods of conducting a battle. The father of modern strategic study, Carl von Clausewitz, defined military strategy as “the employment of battles to gain the end of war”, (LeVeqe, 2006).

Risk is potential damage to an organization’s value, often from inadequate management of processes and events thus impacting on organization’s objectives. IT Risk is emerging as a significant component of total business risk as IT assumes a more prominent role in organizations, and can account for more than 50% of total capital expenditure at some organizations. Information Technology (IT) Risk is a growing component of total Operational Risk. As businesses increasingly depend on IT to automate processes and store information, IT Risk Management is emerging as a separate practice. Organizations across sectors and industries have begun to consolidate functions to develop a more comprehensive, focused approach to IT Risk. IT Risk includes security, availability, performance and compliance elements, each with its own drivers and capacity for harm (Zeid, 2014).

Enterprise risk management is not static, but rather a continuous or iterative interplay of actions that permeate an entity. These actions are pervasive and inherent in the way management runs the business. Business risk is often split into financial and operational components. Information Technology Risk Management is emerging as a separate practice
because of the unique role IT plays in today’s organizations; IT is now integral to many business operations and transactions. In Financial Services, for example, virtually the entire business may be carried out across IT systems and networks. Secondly, IT Risk evolves as fast as technology changes. For example, online “phishing” fraud – and legal and regulatory requirements for IT countermeasures – were virtually unknown just three years ago (Westerman and Walpole, 2005).

Today, the success of organizations and even nations may hinge on mastering a broad landscape of IT risks. The World economic Forum provides a sense of scale. They rank a breakdown of critical information infrastructure among the most likely core global risks, with 10 to 20 percent likelihood over the next 10 years and potential worldwide impact of $250 billion. Sustained investment in IT which is almost $1.2 trillion or 29 percent of 2007 private-sector capital investment in the U.S. alone is fueling growing exposure to IT Risk.

An enterprise IT risk is a potential exposure facing the enterprise as a result of any aspect of the IT environment. This includes IT assets, organization or processes. The four key enterprise risks that are most affected by IT are Availability, Access, Accuracy, and Agility. Three core disciplines - IT foundation, risk governance process, and risk aware culture, constitute an effective risk management capability. According to Zeid (2014), enterprises that build the three core disciplines manage risk more effectively and their business executives have better understanding of their IT risk profile and risk tradeoffs. When done well, IT risk management would mature an organization from a set of difficult compliance and threat-reduction activities to become a true source of agility and business value in the organization.

In view of the background presented in this section, the purpose of this study is therefore to explore ways of managing enterprise IT risk for strategic business value by enhancing tax revenue administration in the context of Less Developed Countries (LDCs).

According to the Kenya Revenue Authority Act (Cap 469), Kenya Revenue Authority was established in 1995 as a semi-autonomous government agency responsible for revenue administration. The overall objective was to provide operational autonomy in revenue
administration and enable its evolution into a modern, flexible and integrated revenue collection agency. The KRA Mission is to promote legitimate international trade through responsible enforcement of the tax laws by a highly motivated and professional team and the application of modern technology.

Since the inception of KRA, revenue collection has continued to grow while professionalism in revenue administration has been enhanced. However, a number of processes remain manual and KRA is yet to operate as a fully integrated organisation. In a bid to fully automate the processes, the KRA Information Communication & Technology (ICT) strategy was developed to act as the blueprint for all future automation programmes. This has seen modernization and automation of processes in the main revenue departments in the authority, and as a result has led to an increase revenue collection. Among the significant challenges reform, modernization and automation process have encountered include lack of sufficient funding, Implementation hiccups in Simba 2005 towards the attainment of a complete self-assessment regime while faster progress is needed in the implementation of an Integrated Tax Management System, stakeholders’ resistance to reform initiatives, need for sustained efforts in fighting corruption and tax fraud, timeliness of legislative changes, human resource issues like remuneration, skills and integrity (KRA Research team, 2012).

1.2 Statement of the Problem

Information technology has become increasingly important part of every enterprise as electronic business has emerged as a strategic imperative for many firms, particularly large organizations. As a result, managing IT risks has become critically important across the enterprise. The complexity of IT has only made it very difficult to understand and make good decisions about IT risks. The causes and effects of IT risk are complex, especially in large organizations. Only a well-defined risk management process can make sense of the complexity (Westerman and Hunter, 2007).

The context of the Less Developed Countries such as Kenya in particular, experience similar challenges and tax revenue loss. In tax revenue administration, according to a research carried out by a Kenya Revenue Authority on the Potential Tax Loss through the ICT (2005),
the country losses about Kshs. 150 million though limitation of data compromised accurate estimation of the same. According to a report by the ECA/IDRC Pan-African Initiative on E-Commerce (2001), there is no process in place in many African countries to review the commercial code to accommodate enterprise technical risk management. As a result, IT Risk Management is gaining visibility across many public and private organizations. Enterprises are considering not only technical risks, but also how IT risks influence enterprise-level risks. The executive’s view of IT risk is moving beyond availability and access management to examine implications of information accuracy and strategic agility. However, few enterprises in the less developed countries are mature in their ability to manage enterprise IT risks. As a result, most enterprises employing an intuitive approach to risk management: as they address high-profile risks that get media attention such as viruses or power outages or wireless, but subsequently miss many risks that are lower-profile such as inadequate internal controls or aging, brittle applications. This growing problem presents the need for a framework for analysis (Westerman and Walpole, 2005).

According to Wyman (2010), despite significant investments in improving their IT risk management capabilities and knowledge advancement in risk identification and assessment methodologies in the recent years, most executives and managers still rate their organizations as "ineffective" or only "moderately effective" at incorporating emerging technological risks into their decision making. The continuing trend to lower the cost income ratio stimulates restructuring of the IT environments and thus leads to new types of risk. From the corporate perspective, a major challenge lies in coping with rapid technological change and the increasing complexity of the IT landscape. At the same time, the restructuring of business processes and application systems is externally triggered by international regulations, such as the International Accounting Standards. These significant changes are further accompanied by the required integration of IT management activities into the operational risk management process. The mentioned internal and external factors are driving forces for operational technology risk management. Naturally, the stronger the influence of IT on a firm’s economic success is, the greater will be the associated risks. This poses new challenges to enterprises with regard to controlling and governing their risks more systematically. The most damaging technology (or IT/system) risks are often “those that are not well
understood”. Given these assertions, the need for innovative approaches and new concepts offering an integrated support is more evident than ever before.

1.3 Purpose of the Study

The purpose of this study is to examine the framework for the management of information technology risks in tax revenue administration for strategic agility using Kenya as a context of Less Developed Countries (LDCs).

1.4 Research Questions

This study sought to accomplish the research purpose through investigation of the following questions in relation to tax revenue administration in developing country, using Kenya as a case of study:

1. What is the nature of information technology risks?
2. What are components of IT risk management and what processes are involved?
3. What are the challenges in IT risk management?
4. How can enterprises formulate enterprise risk management framework to enable the desired strategic agility?

1.5 Importance of the Study

The study sought to explore innovative approaches and new concepts offering an integrated support to enterprise IT risk management for strategic agility in tax revenue administration through the key stakeholders, who are in this case the middle level managers both from the information and communications technology and other revenue departments involved in the management of risks in their respective areas of operations.

1.5.1 Government

By focusing on strategic issues and factors that affect the heart of the tax revenue administration in developing countries, the research will help show how organizations could enhance their ability to deliver and grow, gaining a strategic advantage, rather than seeing risk as only representing physical threats to the business.
1.5.2 Industry
The research will be of importance to the industry in its focus on positive outcomes, enterprise IT risk management should provide a major contribution to those aspects of corporate governance directed to enhance organizational performance.

1.6 Scope of the Study
This study narrowed down on developing countries, focusing on Kenya as a case. A representative sample of information technology and business executives, from Kenya Revenue Authority and other organizations classified as large taxpayers was surveyed to provide insights into the research questions presented, with the time period being the 2013/2014 financial year. The study reviewed the IT foundation, risk governance process, and risk aware culture, all of which constitute a framework for an effective IT risk management system in Kenya Revenue Authority that would give the enterprise strategic agility in revenue administration.

Geographical limitations were overcome by basing the research in Nairobi since the researcher was based in Nairobi. Therefore KRA management staff based at the KRA headquarters and Nairobi region was interviewed.

1.7 Definition of Terms
1.7.1 Risk
According to Reuvid (2008), risk refers to the possibility of an event occurring that will have an impact on the achievement of an organization’s objectives. Reuvid (2008) further states that risk is measured in terms of impact and likelihood

1.7.2 Enterprise Risk Management
Enterprise risk management refers to a structured, consistent and continuous process across the whole organization for identifying, assessing, deciding on responses to and reporting on opportunities and threats that affect the achievement of its objectives (Choudhry, 2006).
1.7.3 Electronic Data Interchange (EDI)
Electronic Data Interchange (EDI) refers to the structured transmission of data between organizations by electronic means. It is used to transfer electronic documents from one computer system to another, i.e. from one trading partner to another trading partner (Lam, 2003).

1.7.4 Tax Revenue
In the context of this study, tax revenue refers to the income accruing from taxation to a government during a specified period of time, usually a year (Simon, 1998).

1.8 Chapter Summary
The purpose of this study will be to examine, in the context of Less Developed Countries, how enterprises can gain strategic agility by looking at a holistic approach to risk management rather than what impacts their ability to deliver and grow, and a framework for an effective enterprise risk management process to mature such risks from a set of difficult compliance and threat-reduction activities to a source of agility and business value. A scope of the study has been given as less developed countries, whereby the study is enterprise IT risk management as a strategic enabler in tax revenue administration, relying on Kenya as a representative case study for developing countries, and Kenya Revenue Authority as a representative enterprise.

The next chapter in this study presents a review of the literature related to the problem. Following this is the research methodology, findings of the study, and finally, a discussion of the problem and conclusions and recommendations.
CHAPTER TWO

2.0 LITERATURE REVIEW

2.1 Introduction

This chapter evaluates recent research studies that have been carried out in the area of enterprise risk management, and information technology risks in particular. Kenya as a developing country serves as a case example.

The research objectives of the study include; 1) the nature of information technology risks and the information technology risk profiles, 2) information technology risk management process and the components, 3) information technology risk management challenges, and 4) how enterprises formulate enterprise risk management framework today to enable the desired strategic agility in the future.

The literature begins with a review on the nature of strategy, information technology and its associated operational risk profiles. Thereafter, the literature evaluates the information technology risk management, components and the processes involved and how these processes fit together incorporating the information technology risks. The literature also looks into the challenges and problems in implementing effective IT risk management system for developing countries in general, and specific case information is provided for India, China and Philippines. The Kenyan situation is also elaborated.

2.2 Nature of Information Technology Risks

Managing risk while addressing regulatory uncertainty has emerged as one of the most critical areas of business operations for today’s global financial services organizations. Recent focus has been on reducing redundancies and streamlining risk-related processes and systems. Organizations are increasingly seeking ways to take a more holistic view of risk, compliance, and governance—one that allows them to add value to their operations and create competitive advantage while also addressing bottom-line efficiencies and redundancies (Lam, 2003).
(IRGC, 2009) defines risk governance deficit as deficiencies or failures in the identification, assessment, management or communication of risks, which constrain the overall effectiveness of the risk governance process. Understanding how deficits arise, what their consequences can be and how their potential negative impact can be minimized is a useful starting point for dealing with emerging risks as well as for revising approaches to more familiar, persistent risks.

Risk governance deficits can occur during risk assessment. Such deficits arise when there is a deficiency of either scientific knowledge or of knowledge about the values, interests and perceptions of individuals and societies. They can also be caused by problems within the processes by which data is collected, analyzed and communicated as knowledge, or result from the complexity and interdependencies within the system at risk. Complexity, uncertainty and ambiguity are thus key challenges for risk assessment (IRGC, 2009).

2.2.1 Link between IT Risks and Overall Business Risks

Based on a survey responses conducted by The Research team, Ernest and Young firm Managing Information Technology Risk (2013), many organizations are focusing on the need to better integrate information technology risk management with their overall risk management program and processes. Business risks range from everyday operational shortcomings to rare cataclysmic failures. The types and levels of risk organizations face vary with their business and preferred risk profile. For example, an entertainment company with many customer-facing systems and a strong brand image might have a very different risk profile than a manufacturer with few externally facing systems but significant trade and design information to protect. And a high-growth financial organization in a developing nation might be more concerned about availability and performance risks as it scales up operations than a financial organization in a more mature market where security and compliance concerns prevail.

(IRGC, 2009) note that knowledge can also help to quantify the levels of risk to be experienced by different individuals and communities. Understanding is equally important. If
knowledge exists but is not understood by decision-makers, stakeholders and the public, risk governance becomes highly vulnerable to error and unpredictability. Accurate knowledge and understanding are essential for effective risk governance. Knowledge is needed to reduce complexity and uncertainty and to understand ambiguity. It is needed to clarify the often confusing interactions between multiple sources of harm, what causes them to become risks, and their potential physical, social and economic consequences (IRGC, 2009).

Symantec Corporation (2012), noted that as IT has become widely and deeply interconnected with business operations, IT Risk has grown to prominence as a component of total operational risk. More than just a specialty area of Operational Risk Management, IT Risk Management is emerging as a separate practice because of the unique role IT plays in today’s organizations; the main reason being that IT is now integral to many business operations and transactions. For example, virtually entire businesses may be carried out across IT systems and networks. And secondly, IT Risk evolves as fast as technology changes. For example, online “phishing” fraud – and legal and regulatory requirements for IT countermeasures – were virtually unknown just three years ago.

Information technology risk—a term describing the risks arising from increased dependency on information technology (IT) systems and digital processes—has become a major challenge for risk managers today. As organizations have implemented complex IT systems to automate much of their businesses, so the risks associated with those systems have risen, ranging from system failure to data leaks and electronic security breaches (Westerman and Walpole, 2005).

According to survey by (Reuvid, 2008), managing those risks creates several new challenges for the management. First, most managers don’t have a technology background, so managing digital risk requires tight collaboration between the risk and IT functions. Second, the same technology that enables firms to digitize their business processes also allows criminals and insiders to commit new forms of fraud and theft. Third, new technologies create new threats, requiring firms constantly to reassess and adapt their strategy for managing digital risk.
2.2.2 Increased in Risk Appetite

According to (Reuvid, 2008), financial industry awareness of risk has increased dramatically due to among other reasons corporate failures - such as Enron and WorldCom in the USA, scandals among Wall Street firms and terrorist attacks. Legislation Sarbanes-Oxley increased the regulatory burden and management attention to risk management. Financial services felt even greater pressure as the success of the industry was highly dependent on the trust of the public. The new attention to risk was reflected in increased attention from regulators.

Organizations in the financial industry are subject to regulatory scrutiny from many angles. They are audited regularly by many parties, including financial market regulators, and even customers and their auditors. To manage both internal and external pressures, most executives are increasingly focusing their attention on risk management. The executives want to understand the extent of each enterprise risk the organization faces. Furthermore they need to clearly articulate how information technology influences the enterprise risks.

(Westerman and Walpole, 2005) notes that all aspects of high-volume financial services organization’s business are highly dependent on information technology. Consequently, the organization’s ability to manage IT-related risks has an important influence over the enterprise risk of the business. Due to its role as the country’s sole tax revenue collector on behalf of the government, any operational or regulatory difficulties at the organization could affect its clients’ processes, its clients’ customers and even the whole financial services industry. It’s paramount for the organization to recognize the opportunity to use risk management as an integral part of its efforts to restructure IT assets and organization with an aim to grow tax revenue base.

On risk appetite, (IRGC, 2009) note that once a risk has been assessed from a scientific perspective and the analysis of concerns and perspectives has been completed, decision-makers must determine whether the risk is acceptable and thus whether it requires specific
risk management. Although acceptability is a value-laden judgment that people may sometimes seek to avoid, it is a necessary one in a sound risk governance framework.

Essentially, thresholds for risk acceptability depend on how risks and benefits are balanced. The valuation of potential benefits on whether this value is related to monetary gain, improved welfare, or moral or ethical considerations is crucial to whether one is willing to accept the associated risk. Although a risk may appear to be acceptable (or even negligible) based on purely probabilistic considerations, segments of the public may consider it unacceptable for a variety of psychological or ethical reasons, as has happened with GMOs in Europe and some applications of nanotechnology in several countries (IRGC, 2009).

Deficits in risk acceptability often occur when organizations and stakeholders fail to define the type and amount of risk that they are prepared to pursue, retain or take (risk appetite) or to take relevant decisions based upon their attitude towards turning away from risk (risk aversion). This implies that, in order to make good risk management decisions (cluster B), organizations and stakeholders need to define their level of tolerance for each risk they face (the organization or stakeholder’s readiness to bear the risk after risk treatment in order to achieve its objectives). In the private sector in particular, risk decisions will have to explicitly state the level of loss that the organization is prepared to accept in its operations (IRGC, 2009).

2.2.3 The Complexity of Interconnected Risk Systems

Where systemic interactions are possible or likely, assessing risk problems without acknowledging this complexity will not be fully informative (Sunstein, 2005). For example, some risk assessments fail to take indirect effects or externalities into account and thus trade-offs in decision-making about complex systems are overlooked. As a result, efforts to reduce risks may create new (secondary) risks, unexpected consequences may occur in areas or sectors other than those targeted, and they may be more serious than the original risk. Finally, risks already believed to have been eliminated “can reappear in another place or in a different form” (Barrand, 2007).
Accurate knowledge and understanding are essential for effective risk governance. Knowledge is needed to reduce complexity and uncertainty and to understand ambiguity. It is needed to clarify the often confusing interactions between multiple sources of harm, what causes them to become risks, and their potential physical, social and economic consequences. Knowledge can also help to quantify the levels of risk to be experienced by different individuals and communities. Understanding is equally important. If knowledge exists but is not understood by decision-makers, stakeholders and the public, risk governance becomes highly vulnerable to error and unpredictability (IRGC, 2009).

According to (IRGC, 2009), there are two types of knowledge which are relevant in assessing and understanding risks. The first type of knowledge is the scientific knowledge about the physical properties of a risk, such as: hazards, exposure and vulnerabilities; the probability of the risk occurring; and, the potential impacts and consequences if it does. The second type of knowledge is the knowledge of risk perceptions and their underlying determinants and consequences, such as: stakeholders’ interests and values; recent coverage of risk in the mass media; and, the social, economic and political consequences of conflict between experts’, decision-makers’ and lay-peoples’ perceptions of risk.

### 2.3 Components of Information Technology Risk Management

In his research, (Westerman and Walpole, 2005) define an enterprise IT risk as a potential exposure facing the enterprise as a result of any aspect of the IT environment. He further notes that this includes IT assets, organization or processes.

According to (IRGC, 2009), insufficient understanding of the potentially multiple dimensions of a risk and how interconnected risk systems can entail complex and sometimes unforeseeable interactions. Interactions among the components of a complex system raise numerous difficulties for risk assessment. It becomes difficult to identify, understand and quantify the “causal links between a multitude of potential causal agents and specific observed effects” [IRGC, 2009]. It is difficult to assess the probability and the consequences
of a risk being realized, especially the rapid spread of damages across geographical, functional boundaries.

### 2.3.1 Enterprise IT Risks

(Westerman and Walpole, 2005) have identified four business risks - Availability, Access, Accuracy, and Agility; that are most affected by IT. The four dimensions of Enterprise IT Risk correspond to four enterprise-level objectives of IT; Agility: This refers to implementing new strategic initiatives, such as completing a major business process redesign or launching a new product/service. Accuracy: Accuracy entails providing accurate, timely and complete information that meets the requirements of management, staff, customers, suppliers and regulators. Access: Means ensuring that authorized people have access to information and facilities they need, and that unauthorized people do not gain access. Availability: Refers to keeping existing processes running, and recovering from interruptions.

(Barrand, 2007) state that each initiative for IT funding, organization, sourcing and technology shapes an organization’s risk profile for the short and long term. The initiative can affect the likelihood of an adverse event, its impact (financial, reputational or otherwise), or both. For example, some firms are implementing “single sign-on” capability, in which people can use a single user ID to access many applications. The move, which is aimed at improving user satisfaction, is also seen as improving risk management.

Unfortunately, in many implementations, this is only partly true. Single sign-on can reduce the likelihood of an intrusion, since security personnel can focus on a single access point, and users are more likely to follow security policy if they have only a single user ID. But, many single-sign-on implementations actually increase the impact of an intrusion, since a single intruder has access to more data. The above illustration shows how IT risk management is much more complex than just implementing technology.

### 2.3.2 IT Risk Factors

(Westerman and Walpole, 2005) at MIT have identified other categories of risk factors which are illustrated in Figure 1 below. It’s paramount that organizations must compartmentalize information, understanding which users should have access to what applications and
information. Policies must be created in keeping with the security/privacy needs of the organization as well as its customers and regulators. Information technology for instance must have staff that can responsively administer user access, and must train all users and vendors in the procedures. By considering each of the six categories of risk factors, managers can avoid missing an important piece of the puzzle.

![Enterprise IT Risk Framework](image)

**Figure 1 : Enterprise IT Risk Framework**

Source: Westerman and Walpole, 2005

These four dimensions of Enterprise IT Risk correspond to the four enterprise-level objectives of IT that are in line with the organization’s corporate objectives (Westerman and Walpole, 2005). They note that many firms fall into patterns where one type of risk (most commonly availability) is prioritized over others. Or, worse, they routinely fail to examine one or more dimensions of risk. Over time, a series of incremental decisions, each one following the firm’s standard practice, leads to a risk profile in which some risks are well controlled while others have huge (and often unknown) exposures. He illustrates risk profiling using a global firm, Global Components Inc. He further in the research defines a risk profile as a tool to communicate the enterprise’s relative risk exposure and tolerance on the four dimensions.
Based on the GCI risk profile above, the blue diamond represents the potential level of risk to the business as a whole, before any risk management is undertaken. The maroon represents the IT component of enterprise risk, along each category. The green inner diamond represents IT risk tolerance, meaning the amount of IT risk that the enterprise chooses to live with. Finally, the beige represents the risk gap—the amount of risk that has not yet been mitigated. To compete in very tough markets, GCI relies on strategic agility enabled by frequently buying and selling firms. To address agility risk, GCI moves each acquired firm to a standard technical infrastructure, but keeps the applications intact and under the control of the business unit manager. According to (Westerman and Walpole, 2005), by standardizing infrastructure the firm reduces costs and somewhat reduces availability risks. By keeping each business unit’s unique applications under the control of the business unit manager, GCI believes it reduces agility and availability risks.

Just like the case of GCI, IT managers in similar organizations are currently identifying initiatives to address the risk gaps in access and accuracy. In keeping with GCI’s decentralized philosophy, these initiatives will not require standardizing all systems globally. Instead, they will involve automatically integrating information from disparate applications, and coordinating, rather than centrally controlling, user access. In addition, senior executives
may choose to ‘live with’ the manual financial process, but add manual controls to ensure financial data integrity (Choudhry, 2006).

Westerman also views risk profile as a negotiating tool. Many disagreements over IT priorities can be traced to differing risk perceptions. Comparing each manager’s perception of enterprise risk exposure (beige diamond) and risk tolerance (green diamond) can resolve disputes and help forge a common direction for the future. In combination with a mature risk management process, the risk framework and risk profile tools can improve risk awareness and reduce IT-related exposures. Awareness of risks enables managers to efficiently prioritize which risks they’ll reduce and, just as importantly, to choose which risks they’ll accept (Westerman and Hunter, 2007).

2.3.3 The IT Risk Management Process
As IT Risk Management gains visibility in the world’s enterprises, firms are considering not only technical risks, but also how IT risks influence enterprise-level risks. Westerman observes that the executive’s view of IT risk is moving beyond availability and access management to examine implications of information accuracy and strategic agility. Effective risk management capability has a number of payoffs. Organizations that manage risk effectively have a better handle on how they are addressing high priority risks and importantly, what risks they are choosing to accept and live with. Such organizations are confident that they are focusing money and effort on risks that really matter. And, they can go after opportunities that other enterprises would find too risky to undertake (Reuvid, 2008).

(Westerman and Walpole, 2005) explore how an enterprise can build risk management capability. In interviews with more than 50 IT managers, Westerman and others found that effective risk management is a cohesive combination of three core disciplines: Risk governance process: complete and effective risk-related policies, combined with a mature, consistent process to identify, assess, prioritize, and monitor risks over time. Risk aware culture: skilled people who know how to identify and assess threats and implement effective risk mitigation. Effective IT foundation: IT infrastructure and applications that have
inherently lower risk because they are well-architected and well-managed. If a firm is severely lacking on any of the three disciplines, it cannot be effective at IT risk management (Westerman and Walpole, 2005).

After the information technology process areas are defined, the organization should identify key indicators (KIs), including Key Risk Indicators (KRIs), Key Performance Indicators (KPIs), and Key Control Indicators (KCIs). The KIs must be articulated for each information technology process area. Ideally, KIs are simple and measurable. KIs may be linked to risks and controls contained in a risk and control library. The library, which presents definitions for all risks and controls, helps ensure that risks and controls are classified and assessed consistently throughout the enterprise (ISACA, 2008). Processes and Operational Procedures—Processes and operational procedures represent the heart of the execution phase of the program and should be directly linked to the appropriate risk management standards. Core risk processes should include: Risk measurements and metrics, Risk assessments, risk control assessments (RCA), and risk control self-assessments (RCSA), Detailed risk analyses, including scenario or threat vulnerability analyses, Risk reporting, Issues risk management, Event capture and loss estimates, Risk mitigation planning, Risk acceptance and exception processes (ISACA, 2006).

Risk management processes should be aligned with legal and regulatory requirements and should include or link to relevant activities such as privacy initiatives, information security, and continuity of business. For large organizations to implement risk processes consistently, they must utilize strong communications, focused change management processes, process guidance, and training (Mayer et al., 2008). Organizations should reassess the vulnerability and compliance technology tools already in place to ensure they have the relevant risk management measurements and reporting capabilities in areas such as threat and vulnerability protection, availability monitoring, and entitlements (Mayer et al., 2008).
2.4 Challenges in IT Risk Management

Revenue administrations currently face a variety of political and administrative challenges, including: fluctuating workloads with diminishing operational resources -“do more with less”; greater expectations from stakeholders; and pressure to meet often-conflicting government political, revenue, trade facilitation, social protection, and national security objectives. Moreover, revenue administrations are increasingly required to integrate their systems and procedures with each other and the sophisticated global logistics networks used by international trade and transport operators. To cope with these pressures and challenges, revenue administrations worldwide are seeking fresh methods, including better ways of using IT, to improve their efficiency and effectiveness. As a result, many customs modernization programs have, over the last decade, included significant computerization components (KRA website, About RARMP, 2011).

According to the revised Kyoto Convention, countries reform existing customs practices to further facilitate the international movement of goods. The adoption of simplified business processes, modern risk management approaches, post-clearance audit controls, and the use of information technology tools by managers are all strongly recommended. As a result, and as part of their reform modernization strategies, East AFRITAC member countries have (to varying degrees) automated their customs processes (Global Facilitation Partnership for Transportation and Trade, 2011).

Kenya has implemented the Gainde 2000 system developed by Senegal. The other regional agencies rely mainly on the Automated System for Customs Data. ASYCUDA customs management system developed by United Nations Conference on Trade and Development and implemented in over 80 countries worldwide. However, it is perceived that in all the countries, the automated systems are largely being used for transactions processing, and their full potential is yet to be exploited. In addition, there are concerns that the regional systems are not responsive to the emerging business needs of modern customs administration, especially in enhancing risk management approaches. The situation has been blamed, partly, on the lack of capacity in the regional customs administrations to fully
understand, manipulate and effectively utilize available IT capabilities. However it has also been argued that the existing regional systems are deficient, especially with regard to their data-mining capabilities and ability to support the ever-increasing demands of modern customs operations (Barrand, 2007).

As a result of the above concerns, regional revenue agencies have recently invested considerable resources developing internal capacity, developing workarounds to support key functions such as valuation and risk management, and explored available options to enhance critical functionalities through technology driven reform and modernization Programs.

2.4.1 Inadequate Knowledge and Understanding on Risk Management
Accurate knowledge and understanding are essential for effective risk governance. Knowledge is needed to reduce complexity and uncertainty and to understand ambiguity. It is needed to clarify the often confusing interactions between multiple sources of harm, what causes them to become risks, and their potential physical, social and economic consequences. Knowledge can also help to quantify the levels of risk to be experienced by different individuals and communities. Understanding is equally important. If knowledge exists but is not understood by decision-makers, stakeholders and the public, risk governance becomes highly vulnerable to error and unpredictability (IRGC, 2009).

2.4.2 Organizational Complacency and Conflicts
According to (Barrand, 2007), another key challenge in risk management is institutional complacency, but a nascent economic recovery and the relatively strong recent performance of the financial sector are emboldening many firms. Risk appetites are growing and there is increasing pressure on organizations to expand and boost earnings. Management of risk is not a purely technical task; it may entail accepting or seeking to resolve fundamental conflicts between individuals, organizational levels, businesses and governments and so on. Broadly speaking, those conflicts may relate to differing interests that are typically tangible or material in nature (such as economic interests), to commonly held beliefs about the nature and the consequences of risks, or to basic values such as social justice or ecological
sustainability. They may also relate to differing ideologies, whether those ideologies are grounded in religion, ethics, philosophy, culture, tradition or politics. Conflicts and tensions can arise at multiple levels, and deficits may occur when the determination of “who is at risk?”, “what are the priorities for response?” and “whose priorities are these?” are not made clear or are the subject of disagreement. The underlying motives that drive conflict may be exaggerated by the concerns or personalities of particular leaders, including the varying levels of trust that people have in them, as well as by how comfortable people are with the processes of negotiation, compromise and compensation (IRGC, 2009).

According to (IRGC, 2009), confusion about the underlying motives of protagonists can occur. For example, advocates with a material interest in the issue may represent their position as rooted in a philosophical principle that cannot possibly be compromised. Likewise, decision-makers may dismiss or even disbelieve a stakeholder’s honest claim that a concern flows from adherence to an unusual religious or ethical belief. It may therefore be a challenge for the risk manager to accurately determine what the motives of stakeholders are. Thus, the imperative of conflict resolution rests to some extent on the manager’s critical need to gather information about the views, interests and ideologies of the key stakeholders. In handling conflicts, it is often crucial to reach out to certain stakeholders. Even if those groups cannot make a technical contribution to the task of risk assessment, their views are a crucial part of the knowledge needed.

2.4.3 Balancing Risk and Cost

Once a risk has been assessed from a scientific perspective and the analysis of concerns and perspectives has been completed, decision-makers must determine whether the risk is acceptable and thus whether it requires specific risk management. Although acceptability is a value-laden judgment that organizations may sometimes seek to avoid, it is a necessary one in a sound risk governance framework. Essentially, thresholds for risk acceptability depend on how risks and benefits are balanced. The valuation of potential benefits (whether this value is related to monetary gain, improved welfare, or moral or ethical considerations) is crucial to whether one is willing to accept the associated risk. Even if the scientific aspects of
risk assessment are sound, there may be a failure by decision-makers to consider variables that influence the acceptability of risk or consumer confidence in a product (Barrand, 2007).

Terminology is not uniform, but an inquiry into risk acceptability is called “risk evaluation” in the IRGC Risk Governance Framework. In addition to the valuation of potential benefits, social scientists have determined that a variety of other variables appears to influence public acceptability of risk, beyond the probability and severity determinations that dominate the scientific assessment of risk. These factors include: whether the risk is incurred voluntarily or is imposed on citizens without their informed consent; whether the risk is controllable by personal action or whether it can be managed only through collective action; whether the risk is incurred disproportionately by the poor, children, or other vulnerable subpopulations; whether the risk is unfamiliar and dreadful; whether the risk results from man-made rather than natural causes; and, whether the risk raises questions of intergenerational equity (IRGC, 2009).

Although a risk may appear to be acceptable (or even negligible) based on purely probabilistic considerations, segments of the public may consider it unacceptable for a variety of psychological or ethical reasons, as has happened with GMOs in Europe and some applications of nanotechnology in several countries. To some extent, the inquiry into risk acceptability draws on the risk perception issues discussed earlier. In some public settings, however, the inquiry is more specific and entails a formal determination of risk acceptability under an explicit statutory or administrative standard. The factors involved in a formal risk-acceptability decision may vary depending upon the legal context.

Deficits in risk acceptability often occur when organizations and stakeholders fail to define the type and amount of risk that they are prepared to pursue, retain or take (risk appetite) or to take relevant decisions based upon their attitude towards turning away from risk (risk aversion). This implies that, in order to make good risk management decisions, organizations and stakeholders need to define their level of tolerance for each risk they face (the organization or stakeholder’s readiness to bear the risk after risk treatment in order to achieve
its objectives) (IRGC, 2009). In the private sector in particular, risk decisions will have to explicitly state the level of loss that the organization is prepared to accept in its operations.

2.5 Technology Risk Management Formulation for strategic agility

ICT is crucial in the consolidation of the routine data processing functions, such as registration of taxpayers, processing of returns and payments, maintenance of taxpayer ledgers, detection of non-filing, stop-filing and non-payment of taxes based on self-assessments. It is also important in routine correspondence with taxpayers. This substantially reduces contact between taxpayers and tax officials, thus minimizing opportunities for rent-seeking behavior (Barrand, 2007).

According to KRA PMBO (2008), at the center of all the reform initiatives is focused and innovative leadership. Strategic leadership is an indispensable component of the CEO’s job description, and cannot be delegated to subordinates. The modern CEO must be prepared to scale the stairs and chew gum at the same time. This calls for constancy to purpose. Shifting paradigms is an extremely uncomfortable for those who have been used to the status quo. This came alive when, at the inception of Gainde 2000 system (also known as SIMBA 2005 System) and Electronic Tax Register, traders went on the rampage calling for the scrapping of these reform initiatives, and insisting that the Commissioner General should be sacked. It took the unwavering resolve and personal support of the Commissioner General to push the reform agenda through.

2.5.1 Effective Technology Risk Mitigation

According to (IRGC, 2009), risk mitigation is a systematic methodology used by senior management to reduce mission risk. Risk mitigation can be achieved through any of the following risk mitigation options which include; risk assumption which means accepting the potential risk and continuing operating the technology system or to implement controls to lower the risk to an acceptable level; risk avoidance which entails avoiding the risk by eliminating the risk cause and/or consequence such as forgoing certain functions of the system or shutting down the technology system when risks are identified.
Other options include risk limitation whereby the risk is limited by implementing controls that minimize the adverse impact of a threat’s exercising a vulnerability such as the use of supporting, preventive, detective controls; risk planning which manages risk by developing a risk mitigation plan that prioritizes, implements, and maintains controls. Research and acknowledgment also lower the risk of loss by acknowledging the vulnerability or flaw and researching controls to correct the vulnerability; and risk transference where the risk is transferred by using other options to compensate for the loss, such as purchasing insurance (IRGC, 2009).

The goals and mission of an organization should be considered in selecting any of these risk mitigation options. It may not be practical to address all identified risks, so priority should be given to the threat and vulnerability pairs that have the potential to cause significant mission impact or harm. Also, in safeguarding an organization’s mission and its IT systems, because of each organization’s unique environment and objectives, the option used to mitigate the risk and the methods used to implement controls may vary. The “best of breed” approach is to use appropriate technologies from among the various vendor security products, along with the appropriate risk mitigation option and nontechnical, administrative measures.

2.5.2 Cost-Benefit Analysis
According to (Barrand, 2007), to allocate resources and implement cost-effective controls, organizations, after identifying all possible controls and evaluating their feasibility and effectiveness, should conduct a cost-benefit analysis for each proposed control to determine which controls are required and appropriate for their circumstances. The cost-benefit analysis can be qualitative or quantitative. Its purpose is to demonstrate that the costs of implementing the controls can be justified by the reduction in the level of risk.

A cost-benefit analysis for proposed new controls or enhanced controls encompasses the following: determining the impact of implementing the new or enhanced controls, determining the impact of not implementing the new or enhanced controls, estimating the costs of the implementation and assessing the implementation costs and benefits against
system and data criticality to determine the importance to the organization of implementing the new controls, given their costs and relative impact (IRGC, 2009).

(IRGC, 2009), further note that the organization will need to assess the benefits of the controls in terms of maintaining an acceptable mission posture for the organization. Just as there is a cost for implementing a needed control, there is a cost for not implementing it. By relating the result of not implementing the control to the mission, organizations can determine whether it is feasible to forgo its implementation.

2.5.3 Continual Evaluation and Assessment of Risk Management

According to (Wyman, 2010), in most organizations, the network itself will continually be expanded and updated, its components changed, and its software applications replaced or updated with newer versions. In addition, personnel changes will occur and security policies are likely to change over time. These changes mean that new risks will surface and risks previously mitigated may again become a concern. Thus, the risk management process is ongoing and evolving.

(Wyman, 2010) further notes that risk management should be conducted and integrated in the SDLC for IT systems, not because it is required by law or regulation, but because it is a good practice and supports the organization’s business objectives or mission. There should be a specific schedule for assessing and mitigating mission risks, but the periodically performed process should also be flexible enough to allow changes where warranted, such as major changes to the IT system and processing environment due to changes resulting from policies and new technologies.

A successful risk management program will rely on (1) senior management’s commitment; (2) the full support and participation of the IT team; (3) the competence of the risk assessment team, which must have the expertise to apply the risk assessment methodology to specific site and system, identify mission risks, and provide cost-effective safeguards that meet the needs of the organization; (4) the awareness and cooperation of members of the user
community, who must follow procedures and comply with the implemented controls to safeguard the mission of their organization; and (5) an ongoing evaluation and assessment of the IT-related mission risks (Wyman, 2010).

For Kenya Revenue Authority, applying risk management in customs and other tax revenue services should aim at effectively preventing and controlling the risk of smuggling and non-compliance. The same as any other kind of management, risk management should also emphasize on maximum security with minimum cost. Thus much determines how organizations should objectively and systematically evaluate the effectiveness of risk management, and thoroughly understands the significance of applying risk management (KRA PMBO, 2008).

Considerations on the strategic aspects of risk management should be made, which means focusing more on reorganizing the management resources of all levels and departments, enhancing the integrity and harmony of risk management, and pushing forward the innovation of system and mode by implementing risk management ideas and methods. The enforcement of risk management must be based on the extensive application of information technologies across the different levels and departments which focus on every process of risk management including data and information collection, risk analysis and assessment, risk treatment, and effectiveness evaluation (KRA PMBO, 2008).

2.6 Chapter Summary

From the literature reviewed in this chapter, building an information technology risk management program is a challenge. But an appropriately designed program helps break down silos and allows the organization to look across functional areas to address risk objectives most effectively.
CHAPTER THREE

3.0 METHODOLOGY

3.1 Introduction

This research design is descriptive in nature. The study aims to examine a detailed framework for the management of information technology risks in tax revenue administration for strategic agility using Kenya as a context of the Less Developed Countries (LDCs).

The population of this study is Kenyan Revenue Authority officials, specifically Information Technology and business executives of the revenue authority. A sample will be chosen from this population set for the purpose of surveying through questionnaires. This chapter outlines the research design, population and sample size, data collection methods, research procedures, data analysis and presentation methods and chapter summary.

3.2 Research Design

The research will be descriptive in nature. According to Cooper and Schindler (2000), a descriptive study is one that is clearly structured with hypotheses and investigative questions. The research objectives that are fulfilled by a descriptive study include descriptions of phenomena or characteristics associated with a particular population, estimates of the proportions of a population that have these characteristics and a discovery of associations among different variables.

The descriptive research design method will be used in this study because it is expected to yield new information and to generate clearer questions and needs identification in terms of what challenges exist in effectively managing Information Technology risks, hence to synthesize emerging knowledge and patterns of effective IT risk management in Kenya and its strategic effects on Tax Revenue administration. Description is used as a tool to organize data into patterns that emerge during analysis (Cooper et. al, 2000).

The topic of this research is ‘Information Technology Risk Management as a Strategic Enabler in Tax Revenue Administration: The Kenyan Context'. Kenya is used as a case
example of Less Developed Countries, where e-commerce is gaining ground fast and so are the digital risks while IT risk management is still nascent and information related to it scanty.

The context of the topic calls for qualitative data gathered on the challenges of management of risks posed by information technology in Kenya and a framework for effective management of the same in tax revenue administration context. Therefore, the conclusions and recommendations of the report will be based on qualitative data and the research objectives are clearly defined, hence, the descriptive research will be used to obtain summary measures to address the research questions.

3.3 Population and Sampling Design

3.3.1 Population
The population for this study will be management and officials from the main departments within the Kenya Revenue Authority, mainly in the middle management positions. Based on the statistics obtained from the Human Resources Department at Kenya Revenue Authority, it has been established that there are approximately 280 members of staff at the supervisory level upwards to the senior management, from across all the departments in Kenya Revenue Authority. This group forms the population of the research study.

3.3.2 Sampling Design and Sample Size
This subsection covers the sample frame, sampling technique and sample size.

3.3.2.1 Sampling Frame
Cooper and Schindler (2000) define a sampling frame as a list of elements from which the sample is actually drawn and is closely related to the population. The sampling frame in this study will consist of IT and business managers in Kenya Revenue Authority. The sampling frame in this research study has been obtained from the target population of senior managers, middle managers and other officials in supervisory levels in all departments within Kenya Revenue Authority.
3.3.2.2 Sampling Technique

A stratified sample will be used to ensure maximum representation of all management staff who in one way or another get involved in the IT risk management process.

3.3.2.3 Sampling Size

Out of the 280 at management level identified as the population in this study, approximately 70% are located in the KRA headquarters, giving a total sampling frame of 160. Only officers at the KRA headquarters will be approached as this area is in close proximity to the researcher. With an acceptable error margin of 5% and a confidence level of 95%, the table below shows how the sample will be drawn from the population for the study.

**Table 1: Table for determining sample size from the given population size**

<table>
<thead>
<tr>
<th>P</th>
<th>S</th>
<th>P</th>
<th>S</th>
<th>P</th>
<th>S</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>10</td>
<td>70</td>
<td>59</td>
<td>160</td>
<td>113</td>
</tr>
<tr>
<td>15</td>
<td>14</td>
<td>75</td>
<td>63</td>
<td>180</td>
<td>118</td>
</tr>
<tr>
<td>20</td>
<td>19</td>
<td>80</td>
<td>66</td>
<td>190</td>
<td>123</td>
</tr>
<tr>
<td>25</td>
<td>24</td>
<td>85</td>
<td>70</td>
<td>200</td>
<td>127</td>
</tr>
<tr>
<td>30</td>
<td>28</td>
<td>90</td>
<td>73</td>
<td>210</td>
<td>132</td>
</tr>
<tr>
<td>35</td>
<td>32</td>
<td>95</td>
<td>76</td>
<td>220</td>
<td>136</td>
</tr>
<tr>
<td>40</td>
<td>36</td>
<td>100</td>
<td>80</td>
<td>230</td>
<td>140</td>
</tr>
<tr>
<td>45</td>
<td>40</td>
<td>110</td>
<td>86</td>
<td>240</td>
<td>144</td>
</tr>
<tr>
<td>50</td>
<td>44</td>
<td>120</td>
<td>92</td>
<td>250</td>
<td>148</td>
</tr>
<tr>
<td>55</td>
<td>48</td>
<td>130</td>
<td>97</td>
<td>260</td>
<td>152</td>
</tr>
<tr>
<td>60</td>
<td>52</td>
<td>140</td>
<td>103</td>
<td>270</td>
<td>155</td>
</tr>
<tr>
<td>65</td>
<td>56</td>
<td>150</td>
<td>108</td>
<td>280</td>
<td>160</td>
</tr>
</tbody>
</table>

**NB:** P=Population size, S=Sample, Confidence level = 95%, Margin of error + or – 5%

3.4 Data Collection Methods

According to Cooper and Schindler (2000), a survey is a primary data collection technique that involves questioning people and recording their responses for analysis. Both secondary data and primary data will be used in the study. Depending on availability, secondary data will be sourced from relevant authorities such as the Kenya Revenue Authority, on any studies that the Research and Corporate Planning Department at Kenya Revenue Authority may have undertaken with regard to information technology business processes automation, modernization and risk management in Kenya. For primary data, the data collection instrument used in this study will be questionnaires. These questionnaires will be used to collect data from managers and tax officials in supervisory levels in the main tax revenue departments and ICT in Kenya Revenue Authority. The questionnaires will be administered via personal visits and e-mail surveys to respondents. The content and layout of the questionnaires for the study will contain a mix of questions allowing both open-ended and specific responses to a broad range of questions.

3.5 Research Procedures

One type of questionnaire will be used in this study. The questionnaire will be developed using the research questions as a basis. Where possible, the questionnaire will be personally administered. Otherwise, email may be used to send the questionnaires to respondents. A prototype version of the questionnaire in this study will be pilot tested on one fifth of the sample before it is improved and sent out to the remaining respondents. The pre-test feedback obtained in the pilot testing will enable a final improved questionnaire to be sent out to the remaining respondents.

3.6 Data Analysis and Presentation

According to Cooper and Schindler (2000), data analysis refers to editing and reducing accumulated data to a manageable size, developing summaries and using statistical techniques for making inferences and conclusions.

In the study, the variables to be examined will be established from the specific research objectives. The statistical software, SPSS will be used to analyze the quantitative data and
results will be presented in graphs, charts, and tables so as to provide a clear picture of the research findings. Quantitative methods will be used to report on the descriptive statistics; these will include analyses of the data in terms of frequencies and measures of central tendency through mean and mode. Qualitative data will be summarized and categorized according to common themes and presented in frequency distribution tables.

3.7 Chapter Summary

Chapter three of the research proposal has covered the research methodology of the study, which is descriptive in nature. The population of this study is Kenyan Revenue Authority officials, specifically Information Technology and business executives of the revenue authority. A sample was chosen from this population set for the purpose of surveying through questionnaires. This chapter outlined the research design, population and sample size, data collection methods, research procedures, data analysis and presentation methods. Questionnaires for the study will be administered to managers of all revenue departments and ICT within Kenya Revenue Authority, based in Nairobi at the Kenya Revenue Authority headquarters. The findings of the study will be presented in tables, graphs and pie charts.
CHAPTER FOUR

4.0 RESULTS AND FINDINGS

4.1 Introduction
The data collected through the questionnaires is explained in this chapter. The findings are presented on the basis of the research objectives, which are; 1) the nature of information technology risks, 2) components of IT risk management and the processes involved, 3) the challenges in IT risk management, and 4) how can enterprises formulate enterprise risk management framework to achieve the desired strategic agility.

Tables, charts and graphs are used to present quantitative data and a brief description of what is shown in the table or figure is provided. A summary of the major findings of the study is provided at the end of the chapter.

A total of forty four management level staff were identified for interviews. Feedback was obtained from the following categories of managers, as shown in table 4:

<table>
<thead>
<tr>
<th>Table 1: Table showing sample size and the respondents interviewed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Department</td>
</tr>
<tr>
<td>Information &amp; Communication Technology</td>
</tr>
<tr>
<td>Customs Services Department</td>
</tr>
<tr>
<td>Domestic Taxes Department – LTO</td>
</tr>
<tr>
<td>Domestic Taxes Department – MTO</td>
</tr>
<tr>
<td>Domestic Taxes Department – DR</td>
</tr>
<tr>
<td>Road Transport Department</td>
</tr>
<tr>
<td>Support Services Department</td>
</tr>
<tr>
<td><strong>Total Valid Cases</strong></td>
</tr>
</tbody>
</table>

Out of the forty respondents interviewed, 36 qualified as valid cases and 4 were identified as cases, but they did not meet the criteria as they had been in the management position for a period of less than 6 months or didn’t have prior management experience.

Of the forty managers interviewed, thirty six responded and were considered valid cases, giving a response rate of 90%. The frequency of how long the managers interviewed had worked with the KRA is depicted in Figure 3 as follows:
Table 2: Respondent’s Length of Service

<table>
<thead>
<tr>
<th></th>
<th>Frequency</th>
<th>Percent</th>
<th>Valid Percent</th>
<th>Cumulative Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid Less than or equal 2</td>
<td>4</td>
<td>11.1</td>
<td>11.1</td>
<td>11.1</td>
</tr>
<tr>
<td>Between 3-5</td>
<td>11</td>
<td>30.6</td>
<td>30.6</td>
<td>41.7</td>
</tr>
<tr>
<td>Between 6-10</td>
<td>21</td>
<td>58.3</td>
<td>58.3</td>
<td>100.0</td>
</tr>
<tr>
<td>Total</td>
<td>36</td>
<td>100.0</td>
<td>100.0</td>
<td>100.0</td>
</tr>
</tbody>
</table>

Figure 3: Showing percentage of respondents length of service

It is clear that the majority of cases (58%) approached to be interviewed had worked with KRA for between 6 to 10 years. This was followed by those who had worked with KRA for between 3 to 5 years (30%) and finally those who had worked for KRA for two or less than two years (11%).

4.2 The nature of information technology risks

The 36 managers were asked in identifying IT risks the sources they consider for strategic and operational risks. Their responses are displayed in the table below. The number of respondents out of 36 is depicted by N.
2.5.2 Strategic Risks

Table 3 Showing strategic risks

<table>
<thead>
<tr>
<th>Strategic risks</th>
<th>Yes</th>
<th>No</th>
<th>Not Sure</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT alliance risks</td>
<td>47.2</td>
<td>33.3</td>
<td>19.4</td>
</tr>
<tr>
<td>IT risk sources reputation</td>
<td>91.7</td>
<td>8.3</td>
<td>0.0</td>
</tr>
<tr>
<td>IT risk sources opportunity</td>
<td>86.1</td>
<td>13.9</td>
<td>0.0</td>
</tr>
</tbody>
</table>

The findings were such that 47.2% of the respondents were able to identify IT alliance risks whereas 33.3% were not able to. The remaining 19.4% of the respondents were not sure. About the IT risk sources reputation, 91.7% of the respondents could identify risks from the sources reputation whereas 8.3% were not able to identify. Lastly 86.1% were able to identify risk sources opportunity while 13.9% could not identify.
4.2.2 Operational Risks

Table 4 Showing operational risks

<table>
<thead>
<tr>
<th>Operational risks</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Financial risks</td>
<td>100</td>
</tr>
<tr>
<td>Project risks</td>
<td>100</td>
</tr>
<tr>
<td>Compliance risks</td>
<td>47</td>
</tr>
<tr>
<td>New work ways</td>
<td>11</td>
</tr>
<tr>
<td>Technological risks</td>
<td>86</td>
</tr>
<tr>
<td>Security breaches</td>
<td>81</td>
</tr>
<tr>
<td>Human risks</td>
<td>19</td>
</tr>
</tbody>
</table>

Figure 5 Showing operational risks

It is clear that majority (100%) of the respondents could identify financial risks and project risks (100%). 86% and 81% of the respondents could identify technological and security breaches. 47% of the respondents could identify compliance risks and lastly 19% could identify human risks.

4.3 components of IT risk management and the processes involved

The 36 managers were asked in identifying IT risks the sources they consider for strategic and operational risks. Their responses are displayed in the table below. The number of respondents out of 36 is depicted by N.
Table 5 Components of IT risks

<table>
<thead>
<tr>
<th>Components of IT Risks</th>
<th>%</th>
<th>No</th>
<th>Not Sure</th>
</tr>
</thead>
<tbody>
<tr>
<td>What can happen</td>
<td>100</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>How and why risk arise</td>
<td>86.1</td>
<td>3.9</td>
<td>-</td>
</tr>
<tr>
<td>Area of impact</td>
<td>100</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Source of risk</td>
<td>100</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

Figure 6 Components of IT risks

From the results, majority were able to identify components of IT risks such as what can happen (100%), How and why risk arise (86.1%), areas of impact (100%) and finally sources of risks (100%)

4.3.1 Security Responsibility

Table 6: IT risks Responsibility

<table>
<thead>
<tr>
<th>Responsibility</th>
<th>Yes</th>
<th>No</th>
<th>Not Sure</th>
</tr>
</thead>
<tbody>
<tr>
<td>CEO</td>
<td>-</td>
<td>88.9</td>
<td>11.1</td>
</tr>
<tr>
<td>Risk board</td>
<td>-</td>
<td>100.0</td>
<td>-</td>
</tr>
<tr>
<td>Chief Information Officer</td>
<td>100.0</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Risk manager</td>
<td>69.4</td>
<td>30.6</td>
<td>-</td>
</tr>
<tr>
<td>All Staff</td>
<td>-</td>
<td>100.0</td>
<td>-</td>
</tr>
</tbody>
</table>
From the results, it is clear that majority (100) said that the chief information officer is the one charged with security matters, 69.4% said the risk manager is the one responsible for this.

### 4.3.2 Presence of Risk Register

**Table 7: Presences of the risk register**

<table>
<thead>
<tr>
<th></th>
<th>Frequency</th>
<th>Percent</th>
<th>Valid Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Yes</td>
<td>31</td>
<td>86.1</td>
<td>86.1</td>
</tr>
<tr>
<td>No</td>
<td>5</td>
<td>13.9</td>
<td>13.9</td>
</tr>
<tr>
<td>Total</td>
<td>36</td>
<td>100</td>
<td>100</td>
</tr>
</tbody>
</table>

**Figure 8: presence of the risk register**
It is clear that majority (86%) agreed that there was presence of risk register whereas 14% said there was no presence of risk register.

### 4.3.3 Risk Register/Database Record Details

**Table 8: The risk register details**

<table>
<thead>
<tr>
<th>Record(s)</th>
<th>Yes</th>
<th>No</th>
<th>Not sure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source</td>
<td>86.1</td>
<td>5.6</td>
<td>8.3</td>
</tr>
<tr>
<td>Nature</td>
<td>86.1</td>
<td>5.6</td>
<td>8.3</td>
</tr>
<tr>
<td>Existing controls</td>
<td>55.6</td>
<td>36.1</td>
<td>8.3</td>
</tr>
<tr>
<td>Consequences and likelihood</td>
<td>-</td>
<td>80.6</td>
<td>19.4</td>
</tr>
<tr>
<td>Initial IT risk rating</td>
<td>22.2</td>
<td>52.8</td>
<td>25.0</td>
</tr>
<tr>
<td>Record Vulnerability</td>
<td>16.7</td>
<td>47.2</td>
<td>36.1</td>
</tr>
</tbody>
</table>

**Figure 9: The risk register details**

86.1% of the respondents were able to identify the source and nature of risks, 55.6% were able to identify existing controls, 22.2% were able to identify initial IT risk rating and 16.7% were able to identify record vulnerability.
4.3.4 Tools and techniques for identifying risks

Table 9: Tools and techniques for identifying risks

<table>
<thead>
<tr>
<th>Tools to Identify Risks</th>
<th>Yes</th>
<th>No</th>
<th>Not sure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit/Physical Inspection</td>
<td>100.0</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Brainstorming</td>
<td>19.4</td>
<td>69.4</td>
<td>11.1</td>
</tr>
<tr>
<td>Overseas experience</td>
<td>-</td>
<td>88.9</td>
<td>11.1</td>
</tr>
<tr>
<td>SWOT</td>
<td>-</td>
<td>88.9</td>
<td>11.1</td>
</tr>
<tr>
<td>Interview/Focus groups</td>
<td>94.4</td>
<td>5.6</td>
<td>-</td>
</tr>
<tr>
<td>Incidences/Scenarios</td>
<td>58.3</td>
<td>41.7</td>
<td>-</td>
</tr>
<tr>
<td>Past experience</td>
<td>100.0</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Process analysis</td>
<td>44.4</td>
<td>55.6</td>
<td>-</td>
</tr>
</tbody>
</table>

Figure 10 Tools and techniques for identifying risks

From the respondents, 100% apply Audit/Physical Inspection, 100% past experience followed by 94.4% interview/focus groups, 58.3% incidences/scenarios and lastly 19.45 apply brainstorming as tools and techniques for identifying risks.
4.4 Challenges In Technology Risk Management

Table 10: Challenges in risk management

<table>
<thead>
<tr>
<th></th>
<th>Frequency</th>
<th>Percent</th>
<th>Valid Percent</th>
<th>Cumulative Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid</td>
<td>Yes</td>
<td>32</td>
<td>88.9</td>
<td>88.9</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>4</td>
<td>11.1</td>
<td>100.0</td>
</tr>
<tr>
<td>Total</td>
<td></td>
<td>36</td>
<td>100.0</td>
<td>100.0</td>
</tr>
</tbody>
</table>

Figure 11: Challenges in IT Risk Management

It is clear from the findings that majority (89%) of the respondents experience challenges in technology risk management whereas 11% don’t.
4.5 Effectiveness of Enterprise IT Risk Management

4.5.1 Partner Impediments in developing Risk Management Plans

Table 11: Partner impediments in developing risk management plans

<table>
<thead>
<tr>
<th></th>
<th>Frequency</th>
<th>Percent</th>
<th>Valid Percent</th>
<th>Cumulative Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Yes</td>
<td>4</td>
<td>11.1</td>
<td>11.1</td>
<td>11.1</td>
</tr>
<tr>
<td>No</td>
<td>21</td>
<td>58.3</td>
<td>58.3</td>
<td>69.4</td>
</tr>
<tr>
<td>Not Sure</td>
<td>11</td>
<td>30.6</td>
<td>30.6</td>
<td>100.0</td>
</tr>
<tr>
<td>Total</td>
<td>36</td>
<td>100.0</td>
<td>100.0</td>
<td></td>
</tr>
</tbody>
</table>

Figure 12: Partner impediments in developing risk management plans

From the results, 58.3% do not have cases of partner Impediments in developing Risk Management Plans whereas 30.6% of those interviewed reported that they are not sure. 11.1% of the respondents said they do have such cases.
4.5.2 Organization review of risk profile

Table 12: Organization review of risk profile

<table>
<thead>
<tr>
<th>Changes</th>
<th>Yes</th>
<th>No</th>
<th>Not sure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Org. structure</td>
<td>5.0</td>
<td>75.0</td>
<td></td>
</tr>
<tr>
<td>Government policy</td>
<td>47.2</td>
<td>47.2</td>
<td>5.6</td>
</tr>
<tr>
<td>Stakeholder relationship</td>
<td>16.7</td>
<td>83.3</td>
<td></td>
</tr>
<tr>
<td>Past experience</td>
<td>100.0</td>
<td>-</td>
<td></td>
</tr>
</tbody>
</table>

Figure 13: Organization review of risk profile

About organization review of risk profile, 100% of the respondents said that the review of organizational risk profile is done based on past experience, whereas 47.2% said this is done based on the government policy, 16.7% based on stakeholder relationship and lastly 5% is done based on the organization structure.
4.5.3 Extent/scope and responsibilities for risk analysis

Table 13: Extent/scope and responsibilities for risk analysis

<table>
<thead>
<tr>
<th></th>
<th>%</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk analysis</td>
<td>Yes</td>
<td>No</td>
<td>Not sure</td>
</tr>
<tr>
<td>Likelihood</td>
<td>75.0</td>
<td>25.0</td>
<td>-</td>
</tr>
<tr>
<td>Consequences</td>
<td>100.0</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Financial impact</td>
<td>100.0</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Reputation</td>
<td>86.1</td>
<td>13.9</td>
<td></td>
</tr>
<tr>
<td>Business objectives</td>
<td>88.9</td>
<td>-</td>
<td>11.1</td>
</tr>
</tbody>
</table>

About the extent/scope and responsibilities for risk analysis, the risks are analyzed in terms of 100% consequences, 100% financial impact, 88.9% business objectives, 86.1% reputation and lastly 75% likelihood of the risk arising.
4.5.4 Analysis of the Risk Difficulties

Table 14: Analysis of risk difficulty

<table>
<thead>
<tr>
<th>Risks Difficult to</th>
<th>Yes</th>
<th>No</th>
<th>Not sure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assess occurrence likelihood</td>
<td>72.2</td>
<td>27.8</td>
<td>0</td>
</tr>
<tr>
<td>Assess potential impact</td>
<td>94.4</td>
<td>5.6</td>
<td>0</td>
</tr>
<tr>
<td>Prioritize</td>
<td>80.6</td>
<td>19.4</td>
<td>0</td>
</tr>
<tr>
<td>Develop/review mitigation strategies</td>
<td>94.4</td>
<td>5.6</td>
<td>0</td>
</tr>
<tr>
<td>Monitor</td>
<td>83.3</td>
<td>16.7</td>
<td>0</td>
</tr>
</tbody>
</table>

Figure 15: Analysis of risk difficulty

4.5.5 Response on risk level for the Last five years

Table 15: Risk level for last 5 years

<table>
<thead>
<tr>
<th>Valid</th>
<th>Frequency</th>
<th>Percent</th>
<th>Valid Percent</th>
<th>Cumulative Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Increased</td>
<td>31</td>
<td>86.1</td>
<td>86.1</td>
<td>86.1</td>
</tr>
<tr>
<td>Decreased</td>
<td>5</td>
<td>13.9</td>
<td>13.9</td>
<td>100.0</td>
</tr>
<tr>
<td>Total</td>
<td>36</td>
<td>100.0</td>
<td>100.0</td>
<td></td>
</tr>
</tbody>
</table>
Figure 16: Risk level for last 5 years

From the respondents, it is evident that majority (86.1%) feel that the response on risk level for the last five years has increased while 13.9% otherwise.

4.5.6 Key Indicators used to monitor different risks

Table 16: Key indicators to monitor organizational risks

<table>
<thead>
<tr>
<th>Indicators to monitor</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>IT risk levels</td>
<td>38.9</td>
</tr>
<tr>
<td>Risk treatment measures</td>
<td>88.9</td>
</tr>
<tr>
<td>Effective of risk treatment measures</td>
<td>38.9</td>
</tr>
</tbody>
</table>

Figure 17: Key indicators to monitor organizational risks
Among the key indicators used to monitor organization risk according to the respondents, risk treatment measures is leading with 88.9%, IT risk levels and effectiveness of risk treatment measures standing at 38.9% each.

4.5.7 Risk management process subject to

4.5.7.1 Internal/external audit

Table 17: Is Risk management process subject to audits

<table>
<thead>
<tr>
<th>Risk Management process subject to</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal audit</td>
<td>Yes</td>
</tr>
<tr>
<td>Internal audit</td>
<td>100</td>
</tr>
<tr>
<td>External audit</td>
<td>61.1</td>
</tr>
</tbody>
</table>

Figure 18: Is Risk management process subject to audits

Majority (100%) of the respondents felt that the risk management process is subjected to internal audit and 61.1% felt that the risk management process is subjected to external audit. 38.9% felt that the risk management is not subjected to external audit.

4.5.7.2 Improved Performance

Table 18: Risk management subject to internal improved performance

<table>
<thead>
<tr>
<th></th>
<th>Frequency</th>
<th>Percent</th>
<th>Valid Percent</th>
<th>Cumulative Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid Yes</td>
<td>36</td>
<td>100.0</td>
<td>100.0</td>
<td>100.0</td>
</tr>
</tbody>
</table>
Majority (100%) of the respondents felt that the risk management process is subjected to internal improved performance as can be attested by the table and graph above.

4.5.8 Overall level of risk management practice development

**Table 19: Overall level of risk management practice development**

<table>
<thead>
<tr>
<th></th>
<th>Frequency</th>
<th>Percent</th>
<th>Valid Percent</th>
<th>Cumulative Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Well Developed</td>
<td>11</td>
<td>30.6</td>
<td>30.6</td>
<td>30.6</td>
</tr>
<tr>
<td>Fairly Developed</td>
<td>16</td>
<td>44.4</td>
<td>44.4</td>
<td>75.0</td>
</tr>
<tr>
<td>Basic</td>
<td>9</td>
<td>25.0</td>
<td>25.0</td>
<td>100.0</td>
</tr>
<tr>
<td>Total</td>
<td>36</td>
<td>100.0</td>
<td>100.0</td>
<td></td>
</tr>
</tbody>
</table>
About the overall risk management practice development, majority (44.4%) of the respondents felt that it is fairly developed, while 30.6% felt that it is well developed. The remaining (25%) felt that it is basic.

4.6 Chapter Summary
Chapter four presented the data that was collected through the questionnaires. The findings were presented on the basis of the research questions. From the findings it emerged that most of the managers interviewed had worked in KRA for over 3 years. Only 11% of the managers interviewed had worked for less than two years.

On the nature of IT risks, the findings were such that 47.2% of the respondents were able to identify IT alliance risks whereas 33.3% were not able to. The remaining 19.4% of the respondents were not sure. About the IT risk sources reputation, 91.7% of the respondents could identify risks from the sources reputation whereas 8.3% were not able to identify. Lastly 86.1% were able to identify risk sources opportunity while 13.9% could not identify.

On the components of IT risks, the majority were able to identify components of IT risks such as what can happen (100%), How and why risk arise,(86.1%) , areas of impact (100%) and finally sources of risks (100%). The majority (100) said that the chief information officer is the one charged with security matters, 69.4% said the risk manager is the one responsible for this.

From the research, the majority (86%) agreed that there was presence of risk register whereas 14% said there was no presence of risk register. 86.1% of the respondents were able to identify the source and nature of risks, 55.6% were able to identify existing controls, 22.2% were able to identify initial IT risk rating and 16.7% were able to identify record vulnerability. From the respondents, 100% apply Audit/Physical Inspection, 100% past experience followed by 94.4% interview/focus groups, 58.3% incidences/scenarios and lastly 19.45 apply brainstorming as tools and techniques for identifying risks.
On the challenges on the risk management process, the majority (89%) of the respondents experience challenges in technology risk management whereas 11% didn’t. About the extent/scope and responsibilities for risk analysis, the risks are analyzed in terms of 100% consequences, 100% financial impact, 88.9% business objectives, 86.1% reputation and lastly 75% likelihood of the risk arising. Among the key indicators used to monitor organization risk according to the respondents, risk treatment measures is leading with 88.9%, IT risk levels and effectiveness of risk treatment measures standing at 38.9% each.

Majority (100%) of the respondents felt that the risk management process is subjected to internal audit and 61.1% felt that the risk management process is subjected to external audit. 38.9% felt that the risk management is not subjected to external audit. Majority (100%) of the respondents felt that the risk management process is subjected to internal improved performance as can be attested by the table and graph above.

On the overall risk management practice development, majority (44.4%) the respondents felt that it was fairly developed, while 30.6% felt that it is well developed. The remaining (25%) felt that it is basic. The next chapter draws interpretations and conclusions from the findings.
CHAPTER FIVE

5.0 DISCUSSION, CONCLUSIONS AND RECOMMENDATIONS

5.1 Introduction
This chapter seeks to draw interpretations and conclusions from the data collected through questionnaires presented in chapter four. It provides a summary of important elements including the purpose of the study and research questions, research methodology used and major findings. The major findings of the study are organized according to the research questions, by comparing the results to the theoretical background presented in the literature review. Thereafter, recommendations are provided for practice, improvement and further studies.

5.2 Summary
The purpose of the study was to examine a detailed framework for the management of information technology risks as a strategic enabler in tax revenue in the context of developing and Less Developed Countries (LDCs). The study used Kenya as a case study. The research questions of the study included the nature of information technology risks, the components of IT risk management and the processes involved. The study also looked at the challenges in IT risk management in the tax revenue administration Kenyan context. It also established an analytical framework for an effective enterprise risk management by organizations to realize the desired strategic agility.

The research methodology was descriptive in nature. The population of this study was Kenyan Revenue Authority management level staff, specifically from Information Technology and revenue departments. A sample size of 44 was identified for interview from a sampling frame of 160. The main data collection instrument used was questionnaires. Four respondents did not return the questionnaires and were non-responsive. The statistical software, SPSS was used to analyze the quantitative data and results were presented in graphs, charts and tables. Quantitative methods to report on the descriptive statistics included analyses of the data in terms of frequencies and measures of central tendency through mean.
and mode. Qualitative data was summarized and categorized according to common themes and presented in frequency distribution tables.

From the findings it emerged that 89% of the managers interviewed had worked in KRA for over 3 years. Only 11% of the managers interviewed had worked for less than two years. On the nature of IT risks, the findings were such that 47.2% of the respondents were able to identify IT alliance risks whereas 33.3% were not able to. The remaining 19.4% of the respondents were not sure. About the IT risk sources reputation, 91.7% of the respondents could identify risks from the sources reputation whereas 8.3% were not able to identify. Lastly 86.1% were able to identify risk sources opportunity while 13.9% could not identify.

On the components of IT risks, the majority were able to identify components of IT risks such as what can happen (100%), How and why risk arise,(86.1%) , areas of impact (100%) and finally sources of risks (100%). The majority (100) said that the chief information officer is the one charged with security matters, 69.4% said the risk manager is the one responsible for this.

From the research, the majority (86%) agreed that there was presence of risk register whereas 14% said there was no presence of risk register. 86.1% of the respondents were able to identify the source and nature of risks, 55.6% were able to identify existing controls, 22.2% were able to identify initial IT risk rating and 16.7% were able to identify record vulnerability. From the respondents, 100% apply Audit/Physical Inspection, 100% past experience followed by 94.4% interview/focus groups, 58.3% incidences/scenarios and lastly 19.45 apply brainstorming as tools and techniques for identifying risks.

On the challenges on the risk management process, the majority (89%) of the respondents experience challenges in technology risk management whereas 11% didn’t. About the extent/scope and responsibilities for risk analysis, the risks are analyzed in terms of 100% consequences, 100% financial impact, 88.9% business objectives, 86.1% reputation and lastly 75% likelihood of the risk arising. Among the key indicators used to monitor
organization risk according to the respondents, risk treatment measures is leading with 88.9%, IT risk levels and effectiveness of risk treatment measures standing at 38.9% each.

Majority (100%) of the respondents felt that the risk management process is subjected to internal audit and 61.1% felt that the risk management process is subjected to external audit. 38.9% felt that the risk management is not subjected to external audit. Majority (100%) of the respondents felt that the risk management process is subjected to internal improved performance as can be attested by the table and graph above.

On the overall risk management practice development, majority (44.4%) the respondents felt that it was fairly developed, while 30.6% felt that it is well developed. The remaining (25%) felt that it is basic.

5.3 Discussion
5.3.1 Nature of Information Technology Risks
The findings of the study revealed that 47.2% of the respondents were able to identify IT alliance risks whereas 33.3% were not able to. The remaining 19.4% of the respondents were not sure. According to the literature review, is critical that organizations are able to understand and appreciate the nature of Information Technology risks they intend to manage if they are to gain business leverage from the risk management process (Lam, 2003).

About the IT risk sources reputation, 91.7% of the respondents could identify risks from the sources reputation whereas 8.3% were not able to identify. As noted in the literature review, the organization’s ability to manage IT-related risks has an important influence over the enterprise risk of the business. Due to its role as the country’s sole tax revenue collector on behalf of the government, any operational or regulatory difficulties at the organization could affect its clients’ processes, its clients’ customers and even the whole financial services industry. It’s paramount for the organization to recognize the opportunity to use risk management as an integral part of its efforts to restructure IT assets and organization with an aim to grow tax revenue base (Westernam and Walpole, 2005).
The findings further revealed that 86.1% were able to identify risks arising from missing opportunities to improve on delivery of the organization’s objectives while 13.9% could not identify such risks. The findings were in line with the information gathered in the literature review where it emerged that managing risk while addressing regulatory uncertainty emerged as one of the most critical areas of business operations for today’s global financial services organizations (Lam, 2003).

The findings of the study confirmed the information gathered in the literature review where it was revealed that most organizations split business risks majorly into financial and operational risks (Economic Intelligence, 2008). This is an area of concern for KRA because whereas financial risks are well understood, Cuske et al. (2007), noted that this approach poses a challenge for operational risks where Information technology risks are categorized under. On operational risks, all of the respondents could identify financial risks and project risks (100%). 86% and 81% of the respondents could identify technological and security breaches as potential sources of operational risks. As noted in the literature review, the research study also affirmed that IT has become widely and deeply interconnected with business operations, IT Risk has grown to prominence as a component of total operational risk. More than just a specialty area of Operational Risk Management, IT Risk Management is emerging as a separate practice because of the unique role IT plays in today’s organizations; the main reason being that IT is now integral to many business operations and transactions. For example, virtually entire businesses may be carried out across IT systems and networks. And secondly, IT Risk evolves as fast as technology changes (Symantec Corporation, 2012).

The study further revealed that 47% of the respondents could identify compliance risks and lastly 19% could identify human risks as sources of risks associated with the delivery of services in the areas of management. The study further confirms the information gathered in the literature review which indicated that IT have become deeply interconnected with business this prominently growing IT risks as a component of total operational risk (Symantec Corporation Research, 2008).
5.3.2 Components of IT Risk Management and Processes Involved

The finding of the study revealed that the majority of the respondents were able to identify components of IT risks. Among the components identified included what can happen if the risk occurred (100%), how the risks could occur and why the risk would arise,(86.1%). As discussed in the literature review, a well-defined, understood identification and analysis process of the IT risks is critical for organizations to gain business leverage from the risk management process (Lam, 2003).

The study also revealed that majority of managers would identify the areas that the risk would impact if it occurred (100%) and this is a very important finding in the sense that during the risk management process, and finally sources of risks (100%). The study further confirms the information gathered in the literature review which indicated that it is paramount that organizations must compartmentalize information where all stakeholders in the organization must be involved and should be aware of their role in risk management (Westerman et al, 2007).

It was clear from the study that majority of the respondents (86%) affirmed that there was a risk register present while 14% of the respondents said there was risk register present. On the information contained in the risk register, 86.1% of the respondents were able to identify the source and nature of risks, 55.6% were able to identify existing controls, 22.2% were able to identify initial IT risk rating and 16.7% were able to identify record vulnerability. The study confirms the information gathered in the literature review that indicated the need for organizations to understand, categorize and document information technology risks in a formal approach that promotes mitigation of those risks thus ensuring continuity (Westerman and Walpole, 2005).

On the tools and techniques used to identify risks, the study revealed that the majority 100% apply Audit/Physical Inspection in identifying risks. Similarly, 100% applied past experience in identifying risks while 94.4% of the managers consider interview and/or focus groups to
identify risks. 58.3% use incidences and scenarios while 19.45% applied brainstorming as tool and techniques for identifying risks.

The study confirms the information gathered in the literature review which indicated that due to the different risk perceptions, using a combination of various tools to identify and manage risks can increase effectiveness, improve risk awareness and reduce IT-related exposures (Hunter, 2007).

5.3.3 Challenges in IT Risk Management Processes

The study clearly revealed that the majority of the respondents experienced challenges in the management of technology risks. Among the challenges identified by the managers included accessing the risk profile or database for existing systems as a basis for mitigation and prevention. Insufficient training and lack of skills on risk management was also cited as a challenge. The majority also identified specific impediments involving external parties or partners in the development of risk management plans. Among the impediments identified included high costs charged for managed security services, the confidentiality concerns of data/information being very critical.

Concerning the organization’s review of risk profile, the findings of the study revealed that 100% of the respondents said that the review of organizational risk profile is done based on past experience, whereas 47.2% said this is done based on the government policy, 16.7% based on stakeholder relationship and lastly 5% is done based on the organization structure. The study findings also revealed that on the extent/scope and responsibilities for risk analysis, all the analyzed risks in terms of consequences and financial impact, 88.9% business objectives, 86.1% reputation and lastly 75% likelihood of the risk arising. The study confirms the information gathered in the literature review which indicated that risks are characterized and analyzed by the severity (or magnitude) of an adverse consequence that can result from an action and the likelihood of occurrence of the given adverse consequence (Barrick, 2007).

From the study findings, it was evident that majority (86.1%) felt that the level of risk the operational areas in the organization has increased for the last five years while 13.9%
otherwise. The findings further support the information gathered in the literature review where it was identified that the level of IT risk is bound to increase due to the increased complexity of IT risks management that result from interdependence of IT and business operations and as a result increasing challenges in the risk management (KRA RARMP Project, 2011).

Among the key challenges identified from the research study is the inability to assess the consequences and likelihood of an identified risk occurring. The majority (86%) of the respondents could not identify the consequence and likelihood while 14% of the respondents were not sure they understood consequence and likelihood. This finding confirms the discussion in the literature review that one of the key challenges is assessing information technology risks (Sunstein, 2005).

5.3.4 IT Risk Management Analytical Framework for Strategic Agility

From the study findings, it emerged clearly that among the key indicators used to monitor organization risk according to the respondents, risk treatment measures was leading with 88.9%, IT risk levels and effectiveness of risk treatment measures stood at 38.9% each.

On the effectiveness of IT Risk management currently in place and the impact on performance and outcomes, the study findings revealed that an effective framework would improve performance through more robust corporate planning, effectiveness in achieving organization’s objectives, improved quality of service delivery to taxpayers and consumers. It was also revealed that an effective risk management framework would lead to increased recognition and uptake of opportunities.

On the overall risk management practice development, the study revealed that majority (44.4%) the respondents felt that it was fairly developed, while 30.6% felt that it is well developed. The remaining (25%) felt that the overall risk management practice development remains fairly basic. This affirms the views in the literature review that ICT is crucial in the consolidation of the routine data processing functions, such as registration of taxpayers, processing of returns and payments, maintenance of taxpayer ledgers, detection of non-filing, stop-filing and non-payment of taxes based on self-assessments. It is also important in
routine correspondence with taxpayers. This substantially reduces contact between taxpayers and tax officials, thus minimizing opportunities for rent-seeking behavior (Barrand, 2007).

Concerning the organization’s review of risk profile, all respondents (100%) agreed that the review of organizational risk profile was done based on past experience as a factor. Similarly, 47.2% said the review was done based on the government policy, while 16.7% based on stakeholder relationship and lastly 5% is done based on the organization structure. The findings of the study confirmed the information gathered in the literature review on the need for constant and regular review of the risk management process (Barrand, 2007).

Majority (100%) of the respondents felt that the risk management process is subjected to internal audit and 61.1% felt that the risk management process is subjected to external audit. 38.9% felt that the risk management is not subjected to external audit. Majority (100%) of the respondents felt that the risk management process is subjected to internal improved performance as can be attested by the table and graph above. On the overall risk management practice development, majority (44.4%) the respondents felt that it was fairly developed, while 30.6% felt that it is well developed. The remaining (25%) felt that it is basic. This confirms from literature review the fact that at the centre of all the reform initiatives, focused and innovative leadership is critical if organizations are to remain agile as they address their IT risks Lam, 200). Strategic leadership is an indispensable component of the management’s job description, and cannot be delegated to subordinates. Shifting paradigms is an extremely uncomfortable for those who have been used to the status quo (KRA PMBO 2008).

5.4 Conclusion
5.4.1 Nature of Information Technology Risks
The causes and effects of IT risk can be complex, especially in large organizations, as it has emerged from the study findings. Without a well-defined risk management process, it can be a very daunting task to make sense of the complexity.
The findings of the study confirmed the information gathered in the literature review that identifying these risks this has posed a challenge for operational risks where Information technology risks are categorized under. On operational risks, all of the respondents could identify financial risks and project risks (100%). 86% and 81% of the respondents could identify technological and security breaches as potential sources of operational risks. The study further revealed that 47% of the respondents could identify compliance risks and lastly 19% could identify human risks as sources of risks associated with the delivery of services in the areas of management.

5.4.2 Components of IT Risk Management and Processes Involved
From the study findings, IT risk management process is complex process. Without a well-defined risk governance process, it would be very difficult to identify, assess and manage IT related risks within any organization. It can also be concluded from the study findings that the risk management process requires an Information security risk conscious culture, that when combined with a mature, consistent process to identify, assess, prioritize, and monitor risks over time is very critical in the entire risk management process. In addition, there is need for a risk aware culture consisting of skilled people who know how to identify and assess threats and implement effective risk mitigation.

5.4.3 Challenges in IT Risk Management Processes
It can be concluded from the study findings that one of the greatest challenges in identifying and assessing risks in tax administration information systems is the complexity of the Kenya Revenue Authority as an organization. The issue of complexity starts with defining the scope and what has to be protected, i.e. in defining the risk management system boundaries.

5.4.4 IT Risk Management for Strategic Agility
From the study findings, it can be concluded that an effective IT risk management capability is an important metric in understanding how IT enables or constrains business initiatives. One can think of strategic agility as a broad concept encompassing the family of business initiatives an enterprise can readily implement. While many elements contribute to an enterprise’s strategic agility, Organizing and coordinating these into an integrated group of
resources results in an enterprise capability. When an organization can perform a capability better than its competitors, that capability becomes its distinctive competency.

5.5 Recommendations

5.5.1 Recommendations for Improvement

5.5.1.1 Nature of Information Technology Risks

Appropriate tools specifically tailored to suit the organization's environment should be developed to harmonize and facilitate identification, classification and documenting of risks. Such tools would also aid and improve the sharing of responsibilities for information security risk management policy in order to better address all the dimensions of IT risks and not just availability and integrity needs.

Secondly, Analytical tools that better capture risk characteristics should be used. Risk assessment tools must be able to capture the potential impact of emerging risks along a broad continuum. Organizations should avoid relying on one-dimensional tools that capture single static events, such as a regulatory change or a competitor’s introduction of a new model.

5.5.1.2 Components of IT Risk Management and Processes Involved

When it comes to the risk management process, responsibility assignment could be improved regarding the identification, assessment and mitigation of Information Technology related risks. In particular, areas such as the co-ordination of risk identification, assessment and mitigation initiatives, the provision of standards and guidelines for risk management and promotion of risk awareness culture within the organization.

Risk metrics should be aligned with performance measures. Developing risk measures based on existing performance measures would have two key benefits; first it would allow the organization to better understand the potential business impact of the risk. Secondly, it draws on terms and measures that are meaningful to the organization, allowing the risk data to be better integrated with strategic and operational decisions. An estimated risk impact that identifies the volatility around a company’s results is far more useful than one that supplies a single, static number.
5.5.1.3 Challenges in IT Risk Management Processes
When considering new initiatives, managers should go beyond return on investment and consider the holistic effect on the enterprise risk profile, as opposed to a single risk dimension. As most Information Technology arrangements affect multiple risk dimensions, decisions should not be made without considering all the risk dimensions. A single dimension of risk, most commonly availability is likely to be prioritized over others this may lead to a risk profile in which some risks are well controlled while others have huge exposures that have not been addressed.

5.5.1.4 Effective IT Risk Management for Strategic Agility
Building an effective enterprise build risk management capability should be a cohesive combination of three core disciplines, Firstly, a risk governance process that should include a complete and effective risk-related set of policies. This should be combined with a mature, consistent process to identify, assess, prioritize, and monitor risks over time. Secondly, risk aware cultures consisting of skilled people who know how to identify and assess threats and implement effective risk mitigation.

Lastly, there is need for an effective IT foundation where IT infrastructure and applications that should have an inherently lower risk as a result of good architecture, well profiled and are well-managed. A performance appraisal process should be elaborated to measure the effectiveness of current information technology risk management processes against current threats for purposes of continuous monitoring, evaluation and improvement.

5.5.2 Recommendations for Further Studies
It is recommended that more research be carried out on analytical framework to integrate emerging risks into the corporate strategy. This is currently a major setback for most organizations, and large ones in particular such as government agencies where KRA falls under. The characteristics of emerging risks, whether external and/or systemic, will often demand significant strategic or operational changes would cushion or minimize their potential impact on the organization as a whole.
REFERENCES


Customs and Excise Act (Cap 472) and related regulations, Laws of Kenya (2000)


Government of Kenya (various): *Budget Speeches*.


IRGC: Risk Governance Deficits: An analysis and illustration of the most Common deficits in risk governance (2009)


Kenya Revenue Authority, Research & Corporate Planning. (2010, July 26). *Risk areas in the KRA*
tax administration system: the case of Customs & Excise and Road Transport Departments in Nairobi


APPENDIX ONE: COVER LETTER FOR QUESTIONNAIRE

Cover Letter for Questionnaire

Muchiri Charles M.
P.O Box 54731 – 00200
Nairobi, Kenya.

To,
Mr. XYZ (The Respondent)
Kenya Revenue Authority
P.O Box 48240 – 00100
Nairobi, Kenya.

dd-mm-yyyy

Dear Respondent (Name),

**Re: Questionnaire – Managing IT Risks for Strategic agility in Tax Administration.**

I am a student at the School of Business, United States International University, Africa. In partial fulfillment of the requirements of the Masters of Business Administration (MBA) program, I am conducting a survey entitled: ‘Information Technology Risk Management as a Strategic Enabler in Tax Revenue Administration: The Kenyan Context’

For this purpose, I have selected you as part of the sample of the population that I intend to study. I will avail the findings of my survey to you upon request.

As a management level staff, you stand to benefit from my study, since I would like to explore how effective management of risks associated with information technology and automation of business processes will give a strategic agility in tax revenue collection. Your recommendations and suggestions will also be highly appreciated.

The information and data is needed for academic purposes only, and will be treated in strictest confidence.
I will greatly appreciate your kind response in filling the questionnaire attached, which will take only a few minutes.

Thanking you and wishing you well,

Yours sincerely,

Muchiri Charles.
Tel: 0722 407886
APPENDIX TWO: QUESTIONNAIRE

Questionnaire

SURVEY STUDY QUESTIONNAIRE

How long have you worked with KRA?

<table>
<thead>
<tr>
<th>No. of Years</th>
<th>Please Tick Appropriately</th>
</tr>
</thead>
<tbody>
<tr>
<td>Less than/equal to 2</td>
<td></td>
</tr>
<tr>
<td>Between 3 - 5</td>
<td></td>
</tr>
<tr>
<td>Between 6 – 10</td>
<td></td>
</tr>
<tr>
<td>Between 11 - 20</td>
<td></td>
</tr>
<tr>
<td>Over 21</td>
<td></td>
</tr>
</tbody>
</table>

1. NATURE OF INFORMATION TECHNOLOGY RISKS

a. Nature of IT risks

In identifying IT risks, does your organization consider the following sources of IT risk:

<table>
<thead>
<tr>
<th>Strategic</th>
</tr>
</thead>
<tbody>
<tr>
<td>● Alliance risk [the risk associated with working with partnering organizations]?</td>
</tr>
<tr>
<td>● Reputation risk [risk of damage to the organization’s credibility and reputation]?</td>
</tr>
<tr>
<td>● Opportunity risks [the risk of missing opportunities to improve on delivery of the Organization’s objectives]?</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Operational [risks associated with delivery of services]</th>
</tr>
</thead>
<tbody>
<tr>
<td>● Financial risk [risks arising from spending on capital projects, fraud]?</td>
</tr>
<tr>
<td>● Project risk [risks of introducing new systems]?</td>
</tr>
<tr>
<td>● Compliance risk [the risk of failing to meet government standards/laws]</td>
</tr>
</tbody>
</table>
and regulations]?

- Risks arising from new ways of working [public – private sector partnerships, outsourcing]?

- Public liability risks [public access, safety]?

- Natural hazard risks?

- Technological risks [innovation, obsolescence, explosions and dependability]?

- Human risks [strike by employees, loss of key personnel]?

- Security risks [premises/computer breaches]?

- Risks arising from pilot projects [risk of not learning from pilots]?

- Other? *(please specify below)*


2. COMPONENTS OF IT RISK MANAGEMENT AND WHAT PROCESSES ARE INVOLVED

a. Does your organization identify risks in terms of:

- What can happen?

- How and why IT risks arise?

- Area of impact?

- The source of the IT risk?
b. Who is responsible for identifying the IT related risks facing your organization [the]:

- Chief Executive Officer? 
- Board/Executive Management Team? 
- Chief Information Officer? 
- Risk Manager? 
- Line Managers? 
- All Staff? 
- Other? *(please specify below)*

---

c. Does your organization have an IT related risk register/database?  

---

d. If **Yes**, in respect of each identified IT risk, the risk register/database records:

- source? 
- nature? 
- existing controls? 
- consequences and likelihood? 
- initial IT risk rating?
• vulnerability to external/internal factors?

• other? (please specify below)

____________________________________________________________________________________________
____________________________________________________________________________________________
____________________________________________________________________________________________

e. What tools and techniques are used by your organization for identifying risks:

• audits or physical inspection?

• brainstorming?

• examination of local/overseas experience?

• SWOT (strengths, weaknesses, opportunities, threats) analysis?

• interview/focus group discussion?

• judgmental?

• surveys/questionnaires?

• scenario analysis?

• operational modeling?

• past organizational experience?

• process analysis?

• other? (please specify below)

____________________________________________________________________________________________
____________________________________________________________________________________________
3. **CHALLENGES IN TECHNOLOGY RISK MANAGEMENT**

<table>
<thead>
<tr>
<th></th>
<th>Yes</th>
<th>No</th>
<th>Not Sure</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. Are there any challenges that you experience during the process of managing or dealing with technology risks that affect your area of management?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>b. If <strong>Yes</strong>, please briefly highlight the challenges you encounter</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>i)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ii)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>iii)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>iv)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>v)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>vi)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>vii)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>viii)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>c. Are there any other specific impediments to involving partners in the development of risk management plans?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>d. If <strong>Yes</strong> please specify</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>e. Does your organization review, and where necessary amend, its risk profile resulting from:</td>
<td>Yes</td>
<td>No</td>
<td>Not Sure</td>
</tr>
<tr>
<td></td>
<td>changes in organizational structure?</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>changes in organization’s role?</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
f. This section seeks to establish the extent/scope and responsibilities for risk analysis, evaluation and treatment in your organization.

<table>
<thead>
<tr>
<th>Are risks analyzed in terms of:</th>
<th>Yes</th>
<th>No</th>
<th>Not Sure</th>
</tr>
</thead>
<tbody>
<tr>
<td>• likelihood?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• consequence?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• financial impact?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• reputation impact?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• achievement of objectives?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• other? <em>(please specify below)</em></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>____________________________________________________________________</td>
<td></td>
<td></td>
<td>----------</td>
</tr>
<tr>
<td>____________________________________________________________________</td>
<td></td>
<td></td>
<td>----------</td>
</tr>
<tr>
<td>____________________________________________________________________</td>
<td></td>
<td></td>
<td>----------</td>
</tr>
<tr>
<td>g. The risks your organization faces are difficult to:</td>
<td>Yes</td>
<td>No</td>
<td>Not Sure</td>
</tr>
<tr>
<td>• assess in terms of occurrence likelihood</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• assess in terms of potential impacts</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• prioritize</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
- develop and review risk mitigation strategies
- monitor.

h. In the last 5 years the level of risk faced by your organization has:

- Increased
- Decreased
- Not Changed
- Not Sure

4. FORMULATING ENTERPRISE RISK MANAGEMENT FRAMEWORK FOR STRATEGIC AGILITY

a. Does your organization have key indicators to routinely monitor the:

<table>
<thead>
<tr>
<th></th>
<th>Yes</th>
<th>No</th>
<th>Not Sure</th>
</tr>
</thead>
<tbody>
<tr>
<td>levels of IT risk?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>application of the IT risk treatment measures?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>effectiveness of the IT risk treatments?</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

If Yes please specify the key performance indicators being used
________________________________________________________________________
________________________________________________________________________
________________________________________________________________________
b. Are the IT risk management processes within your organization subject to audit or other quality assurance mechanism:

<table>
<thead>
<tr>
<th></th>
<th>Yes</th>
<th>No</th>
<th>Not Sure</th>
</tr>
</thead>
<tbody>
<tr>
<td>internal audit?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>external audit?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>other party etc? (please specify below)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

c. Has IT risk management improved performance and or outcomes in the following areas:

<table>
<thead>
<tr>
<th></th>
<th>Yes</th>
<th>No</th>
<th>Not Sure</th>
</tr>
</thead>
<tbody>
<tr>
<td>more robust corporate planning?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>achievement of objectives?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>development of public policy?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>quality of service delivery?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>resource allocation and utilization?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>information systems?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>management reporting?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>communication in the organization?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>development of a risk aware culture in the organization?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>management of stakeholders and customers?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>organizational change?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>reputation management?</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
- public perceptions?
- increased recognition and uptake of opportunities?
- physical asset management?
- recurrent budget management?
- project management?
- accountability requirements?
- other? [please specify]

<table>
<thead>
<tr>
<th>d. Overall, at what stage of risk management practice development does your organization consider itself to be at?</th>
</tr>
</thead>
<tbody>
<tr>
<td>[1 is in line with best practice, 5 is non-existent]?</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Best Practice</th>
<th>Well developed</th>
<th>Fairly developed</th>
<th>Basic</th>
<th>Non existent</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
</tbody>
</table>

NB: Please note that you may give your answers to any of the questions on a separate piece of paper in case the space provided is absolutely limiting.

Thank you for your time and help in this research project

THE END