BINDURA UNIVERSITY OF SCIENCE EDUCATION

RESEARCH TOPIC

ICT RISK MANAGEMENT IN ZIMBABWE: A CASE STUDY OF THE CENTRAL GOVERNMENT'S PUBLIC FINANCIAL MANAGEMENT SYSTEM (PFMS)

SUBMITTED BY

TENDAI KNOWLEDGE MUDZIMUIREMA

IN PARTIAL FULFILMENT OF THE REQUIREMENTS OF THE MASTERS IN BUSINESS LEADERSHIP DEGREE

STUDENT NUMBER : B 1234494

SUPERVISOR : MR. C. MASANGO

FEBRUARY : 2015
RELEASE FORM

Name of Author: Mudzimuirema Tendai Knowledge


Program for which dissertation was presented: Masters in Business Leadership Degree

Year degree granted: 2015

Permission is hereby granted to Bindura University of Science Education Library to produce single copies of this dissertation and to lend or sale such copies for private scholarly or scientific research purposes only. The author reserves other publication rights and neither the dissertation nor extensive extracts from it may be printed or otherwise reproduced without the author’s written permission.

Signed:

Permanent address: Chirombo Village, Domboshava, Goromonzi

Email address: mudzimuirema@yahoo.com

Cellphone: 0772 486 338

Date: 28 February 2015
The undersigned satisfy that they have read and recommend to Bindura University of Science Education for acceptance, a dissertation with the title “ICT Risk Management In Zimbabwe: A Case Study of the Central Government’s Public Financial Management System (PFMS).” by Tendai Knowledge Mudzimuirema in partial fulfilment for the requirements of the degree of masters in business leadership.

Student: …………………………………… ........................................

Signature .................................................. Date

Supervisor: …………………………………… ........................................

Signature .................................................. Date

Program Coordinator: …………………………………… ........................................

Signature .................................................. Date

Faculty Chairman: …………………………………… ........................................

Signature .................................................. Date

External Examiner: …………………………………… ........................................

Signature .................................................. Date
ABSTRACT

This research sought to evaluate the Information Communication Technology risk management practices within Zimbabwe Central Government’s Public Financial Management System Environment through analysing the National ICT Policy, ascertaining the current profiles of ICT risk management within the central government’s PFMS environment and establishing ICT risk management gaps within the central government’s ICT Risk Management Framework. The research adopted an exploratory research design which provided the researcher with better ideas and insights into broader and vague problems concerning ICT risk management within central government’s PFMS environment. In addition exploratory design was appropriate to the current research as it aims at identifying the important and critical determinants of successful ICT risk management within the PFMS environment. The research was therefore focused on ICT risk management in relation to the adequacy of the policies and procedures currently in use as well as the adequacy of the infrastructure, in terms of how this affected successful ICT risk management. The research established that the current policy focuses on e-Readiness and e-Awareness but fails to capture the pertinent issues such as the tremendous telecommunications sector developments and the impediments to ICT sector further growth while the draft reviewed policy that awaits Cabinet approval comprehensively provides strategic direction and guidance for sustainable national ICT development through the development and application of ICTs in Zimbabwe. Most of the ICT and IS risks within the PFMS environment emerged from poor access rights management, inconsistent application of ICT and IS security controls as well as the ministry’s inability to provide essential training to staff fast enough so as to enable them to catch up with the dynamic technological environment. There is need to develop a comprehensive risk assessment framework to enable the conducting of risk assessments on a regular basis. ICT resources also need to be appropriately classified while Service Level Guarantees need to be signed with the vendor companies that the ministry signed Service Level Agreements with. It is critical that both new and existing ICT risk management policies and procedures are operationalised within the PFMS environment. More ICT risk management policies need to be developed in all areas of operations that currently do not have ICT risk management policies. All change initiatives need to be communicated to the stakeholders.
ACKNOWLEDGEMENTS

This study would not have been possible without the help, support and encouragement of many people who assisted me in various and priceless ways in the preparation of this dissertation report.

Dr. S. Kundishora, the Permanent Secretary and Mr. S.C. Chigwamba, the Principal Director, in the Ministry of Information Communication Technology, Postal and Courier Services, to whom I am greatly indebted and sincerely grateful, for according me the opportunity to undertake this study and program.

Mr C. Masango, my lecturer and supervisor, for his most valuable suggestions, comments and guidance during the preparation and writing of this dissertation. This study would not have been what it is today without his selflessness.

My sincere appreciation also goes to the management and co-workers within the Ministry of Information Communication Technology, Postal and Courier Services, for their tolerance and understanding over the period of the study.

Finally, I extend my thanks to the Dean, the lecturers and staff of the Faculty of Commerce at Bindura University of Science Education and my colleagues on the Masters in Business Leadership Degree Program, for their friendliness without which academic life would have been lonely and unbearable.
Table of Contents

RELEASE FORM ............................................................................................................................................... ii
APPROVAL FORM ........................................................................................................................................ iii
ABSTRACT .................................................................................................................................................... iv
ACKNOWLEDGEMENTS .............................................................................................................................. v
Table of Contents .......................................................................................................................................... vi
CHAPTER I ...................................................................................................................................................... 1
INTRODUCTION............................................................................................................................................. 1
1.0. Introduction ........................................................................................................................................... 1
1.1. Background .......................................................................................................................................... 1
  1.1.1. Political Landscape ....................................................................................................................... 3
  1.1.2. Economic Landscape .................................................................................................................... 4
  1.1.3. Technological Landscape ........................................................................................................... 4
  1.1.4. Environmental Landscape ........................................................................................................ 5
  1.1.5. Legal Landscape .......................................................................................................................... 5
1.2. Statement of the research problem ..................................................................................................... 5
1.3. Research objectives ............................................................................................................................. 6
1.4. Research questions .............................................................................................................................. 7
1.5. Justification of the study ..................................................................................................................... 7
1.6. Significance of the study ..................................................................................................................... 8
1.7. Assumptions of the research .............................................................................................................. 9
1.8. Delimitations of the study .................................................................................................................. 9
1.9. Limitations of the study ..................................................................................................................... 10
1.10. Chapter Summary ............................................................................................................................ 10
CHAPTER II .................................................................................................................................................. 11
LITERATURE REVIEW ............................................................................................................................... 11
2.0. Introduction .......................................................................................................................................... 11
2.1. Overview of risk management ......................................................................................................... 11
2.2. Success factors in ICT risk management ......................................................................................... 19
2.3. Identification of sources of ICT risk ................................................................. 20
2.4. Applying ICT risk management concepts .......................................................... 24
2.5. Tools that can be identified in compiling the ICT risk management framework ....... 27
   2.5.1. ICT Governance policy ............................................................................. 27
   2.5.2. Management of Information Technology Security (MITS), Procedures ........ 32
   2.5.3. Management ICT risk management plans .................................................. 36
   2.5.4. Operational ICT risk management plans and procedures ......................... 38
2.6. Chapter Summary ............................................................................................... 40

CHAPTER III .............................................................................................................. 41
RESEARCH METHODOLOGY ....................................................................................... 41
3.0. Introduction .......................................................................................................... 41
3.1 Research Paradigm ............................................................................................... 41
3.2. Selected Research Philosophy .......................................................................... 42
3.3. Research Design ................................................................................................ 43
3.4. Data Collection ................................................................................................... 44
   3.4.1. Depth interviews ...................................................................................... 44
   3.4.2. Questionnaire .......................................................................................... 45
      3.4.2.1 Questionnaire design ............................................................................ 46
      3.4.2.2. Structure of the questionnaire .............................................................. 46
      3.4.2.3. Pre-testing of the questionnaire ............................................................ 46
3.5. Document analysis/review ................................................................................. 47
3.6. Target population ............................................................................................... 48
3.7. Sample size ........................................................................................................ 48
3.8. Sampling procedure used in this study ............................................................... 49
3.9. Research Data Validity and Reliability ............................................................... 49
3.10. Data processing, analysis and presentation ....................................................... 50
3.11. Ethical Considerations ...................................................................................... 50
3.12. Chapter Summary ............................................................................................. 51

CHAPTER IV ............................................................................................................... 52
DATA PRESENTATION AND ANALYSIS .................................................................... 52
4.0. Introduction..................................................................................................................... 52
4.1. Survey response rate........................................................................................................ 52
4.2. Respondent statistics by position level and department worked in............................. 53
4.3. Success factors in ICT risk management within the PFMS Environment....................... 53
  4.3.1. National ICT Governance Policy ............................................................................. 53
  4.3.2. Organisational structure.......................................................................................... 54
  4.3.3. Organisational processes ....................................................................................... 56
  4.3.4. Organisational ICT strategies ................................................................................ 57
    4.3.4.1. Strategic Plan .................................................................................................... 57
    4.3.4.2. Risk Assessments ............................................................................................. 58
    4.3.4.3. Business continuity plan ................................................................................... 58
    4.3.4.4. Standards and Framework Implementation ....................................................... 59
4.4. Identification of sources of ICT and IS risks within the PFMS environment.................. 60
  4.4.1. Pirated software ....................................................................................................... 60
  4.4.2. Information security awareness .............................................................................. 61
  4.4.3. Data input validation ............................................................................................... 62
  4.4.4. Human resources .................................................................................................... 63
  4.4.5. ICT risk awareness ................................................................................................ 63
  4.4.6. System access rights management ........................................................................... 64
  4.4.7. ICT infrastructure and technology within the PFMS environment.......................... 65
4.5. Tools that can be identified in compiling the ICT risk management framework for the PFMS................................................................................................................................. 66
  4.5.1. Strategic level plans................................................................................................. 66
  4.5.2. Operational level plans ........................................................................................... 67
4.6. Chapter Summary............................................................................................................ 69
CHAPTER V ................................................................................................................................ 70
CONCLUSIONS AND RECOMMENDATIONS ........................................................................ 70
5.0 Introduction...................................................................................................................... 70
5.1 Summary of research findings.......................................................................................... 70
5.2. Conclusions ................................................................................................................... 72
5.2.1. To analyse the government ICT Policy that governs the use of ICTs in Zimbabwe in terms of its appropriateness in addressing ICT risk management issues within the PFMS environment. .......................................................................................................................... 72

5.2.2. To ascertain the current profiles of ICT risk management within the central government’s PFMS environment. .......................................................................................................................... 73

5.2.3. To determine ICT risk management gaps within the central government’s ICT Risk Management Framework for the PFMS. .................................................................................................................. 73

5.2.4. General conclusions .......................................................................................................................................................... 73

5.3. Recommendations ........................................................................................................................................................................ 74

5.3.1. ICT risk management strategy and policy issues .......................................................................................................................... 74

5.3.2. Human resources management and planning issues .................................................................................................................. 75

5.3.3. Regulatory compliance and corporate governance (security) issues .......................................................................................... 75

5.3.4. Business continuity management ............................................................................................................................................ 75

5.4. Recommendations for further research ........................................................................................................................................ 76

References ............................................................................................................................................................................................ 77

APPENDICES .................................................................................................................................................................................... 80

Appendix “B” Letter of invitation to participate in the study ........................................................................................................... 80

Appendix “C” PFMS user questionnaire ........................................................................................................................................ 81

Appendix “D” PFMS user Indepth Interview Guide ......................................................................................................................... 86

Figure 4.1 Current Organisational Structure .................................................................................................................................. 89

Figure 4.2: Proposed Organisational Structure ............................................................................................................................... 90
List of Figures

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Figure 4.1</td>
<td>Current Organisational Structure</td>
<td>89</td>
</tr>
<tr>
<td>Figure 4.2</td>
<td>Proposed Organisational Structure</td>
<td>90</td>
</tr>
</tbody>
</table>
# List of Appendices

<table>
<thead>
<tr>
<th>Appendix</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appendix “B” Letter of invitation to participate in the study</td>
<td>80</td>
</tr>
<tr>
<td>Appendix “C” PFMS User questionnaire</td>
<td>81</td>
</tr>
<tr>
<td>Appendix “D” PFMS user Depth Interview Guide</td>
<td>86</td>
</tr>
</tbody>
</table>
1.0. Introduction

This study is on ICT risk management as it pertains to the Zimbabwe Central Government’s Public Financial Management System (PFMS) environment. Whilst the Central Government is no exception in terms of experiencing the benefits that accrue from use of information and communication technologies (ICTs), it is also equally affected by the risks that come with the adoption of ICT applications.

1.1. Background

The Government of Zimbabwe (GOZ) introduced the (PFMS) in 1999, the objective being to improve on accountability and transparency with regard to the ways with which it raises and allocates financial resources for the benefit of the of public. The PFMS is an Enterprise Resource Planning System (ERPS) used to capture, process, discover and compile accurate and real time planning, programming, budgetary, financial accounting and acquisition information for use by decision makers. The system therefore links Treasury with all line ministries thereby enabling Treasury to monitor, supervise and control national spending and revenue inflows across all ministries and their departments throughout the country.

According to the PFMS Implementation Concept Paper (1997), implementation of the system was a result of the GOZ having engaged Ernst and Young as consultants, to prepare the Statement of User Requirements (SOURS) in 1997. The same company was also then appointed as Project Advisors over the period 1998 to 1999. This combined effort lead to the selection of the Turkey Solution provider, Systems Application Products (SAP), the basis upon which the PFMS is developed. Worth noting, as stated in the New System Concept Paper (1997), Central Government was facing numerous financial administrative problems associated with the predecessor system which had been in operation from as way back as the late 1970’s.
The implementation of the PFMS was therefore necessitated by weaknesses in budget executions and accounting processes which were semi-automated, fragmented and often supported by very old and inadequately maintained applications. Consequently, there was lack of reliable and timely revenue and expenditure data for meaningful budget planning, monitoring, expenditure control and status reporting. Cases of fraudulent activities also took long to uncover (The Comptroller and Auditor General reports 1997:1998:1999). Resultantly, there was poorly controlled commitment of public resources evidenced by large build-ups in debt and excessive government borrowings. This also further resulted in fluctuating interest rates coupled with crowding out of private sector investments. Resource misallocations were also rampant thereby negatively impacting on the effectiveness and efficiency with which services were delivered to the nation (World Bank Report 2010).

Implementation of an Enterprise Resource Planning System requires substantial initial investment by the implementing government/organisation. Countries such as Malawi, Zambia and Rwanda started implementing their Integrated Financial Management Systems after having secured donor assistance. On the other hand, it is worth noting that Zimbabwe is the only country, the world over, to have embarked on implementing a PFMS without donor assistance and as such has been experiencing many financial related problems with respect to this exercise. However, the African Development Bank (AfDB) and the United Nations Development Fund started providing system implementation support in July 2010. This assistance has been in the form of capital and technical assistance as well as knowledge transfer. In addition, history has shown that the government has been unable to retain competent staff for most of its senior positions due to its generalised inability to offer competitive remuneration packages compared to the private sector. The Zimbabwean Government has therefore been the training ground for the private sector. The situation government finds itself in is further compounded by the skills flight to supposedly greener pastures abroad, that has been witnessed over the past two decades.

The PFMS is currently rolled out to the Provincial level and Government’s intention is to further cascade the system down to the District level. As such, the user base is quite significant and will continue to grow as the system is rolled out. Whilst the central government will continue to reap
the benefits that accrue from use of information communication technologies (ICTs), the risks that come with the adoption of ICT applications also continue increasing. As a result, effective access controls become critical so as to ensure that the data contained within its systems are duly safeguarded and secured from unauthorized access and manipulation.

The Ministry of Information Communication Technology, Postal and Courier Services (MICTPCS) is mandated to provide and maintain an enabling Information Technology (IT) platform from which the Ministry of Finance and Economic Development (Treasury) operates. The Treasury, with the support from MICTPCS has responsibilities that include desktop support, IT security, database administration, release management, certification, IT resources management and access control. In general, access to the system is controlled by the Treasury. However, the Civil Service Commission (Human Resources Branch) and the Ministry of Home Affairs, whose departments include the Registrar General’s Office and the Immigration Department (e-Government) have some responsibilities for system access related to certain administration specific IT systems such as Immigrants Registration and Births and Deaths Registration respectively. All these systems ride on the PFMS backbone.

ICT governance, like any form of governance, is meant to strategically support and simplify governance for all parties, that is, citizens, enterprises and the government. The efficient use and legislation of ICTs will not only connect all these parties and effectively support their processes, but also increase investment and drive the country towards a more technologically apt society. Therefore, to be able to see the fruits of how ICT can benefit all levels, a practical legal framework that focuses on control and accountability as well as performance and risk management needs to be established and put into practise. This therefore calls for an assessment of the external environment in which the impact of the use of ICTs will be felt.

1.1.1. Political Landscape

The political environment has been relatively stable since the establishment of the Government of National Unity (GNU) in 2009. The environment continues to improve and it has since then
been government policy to equip legislators with laptops. In addition, some of the senior
government officials have been enabled to access the PFMS Network from their homes.
Accessing the PFMS therefore grows the user base, further enabling user visits to undesirable
sites which are the sources of many of the reported viruses. Such user behaviour will therefore
compromise system performance.

1.1.2. Economic Landscape

Zimbabwe has experienced a stable macroeconomic environment with relatively strong GDP
growth rates since 2009. GDP growth had been projected to be on an upward trend since the
introduction of the multi currency regime in early 2009. However, the economy took a dip in
2012 largely due to inherent political and economic uncertainties, a high debt overhang and
deteriorating infrastructure. Projected GDP improvement for 2014 was expected to emanate from
improvements in the mining and agriculture sectors. In order to continue realising GDP growth,
ICT use will also have to increase as most businesses take their places in the global economy.
South Africa remains Zimbabwe’s main trading partner, accounting for more than 60% of
Zimbabwe’s international trade volumes. Within the wholesale and retail trades, 60 - 70% of the
stock on supermarket shelves is of foreign (and mostly South African) origin. This implies that
there is need to improve communication systems between the two countries.

1.1.3. Technological Landscape

Consumer communication technologies continue to develop due to ICT friendly government
policies. The suspension of customs duties on the importation of ICT devices has made laptop
computers, tablets and smart mobile phones accessible to most Zimbabweans.

All government ministries now have each established a website. The public, the international
community included, can now log into these websites and make enquiries with regard to services
offered. These websites are extranets sitting on the PFMS backbone. The literature on ICT risk
management indicates that risks increase with the increased adoption of ICT in business.
1.1.4. Environmental Landscape

Due to the rapid advancement in ICTs, electronic communication gadgets fast become obsolete. There is therefore need to have policies that govern the disposal of such equipment. For example, sanitisation of computers prior to disposal will assist in maintaining the integrity of government information systems and the environment.

1.1.5. Legal Landscape

Most ICT related risks emerge from poor ICT risk management processes. For example, ICT risk is a result of uncontrolled practices that include the use of pirated applications and software, improper or incomplete software licensing and poor protection of intellectual property. Issues regarding cyber security, protection of data, intellectual property rights (IPRs), broadband, e-transactions and ethical and moral rights will require the development of the requisite governance frameworks. This suggests that in the current study, the researcher will need to review the policy that governs the use of ICTs in Zimbabwe in order to ascertain whether it covers these ICT risk management issues.

1.2. Statement of the research problem

Use of ICTs is now respected as one of the major business drivers for central government. The efficiency and effectiveness of government operations will therefore depend on the robustness of the technology and systems in place. Whilst the Central Government is no exception in terms of experiencing the benefits that accrue from use of information and communication technologies (ICTs), it is also equally affected by the risks that come with the adoption of ICT applications. The central government’s PFMS user base continues to grow as the system gets rolled out to different government offices throughout the country. Extranets to enable enquiries into ministerial websites further widens the user base. Such a scenario illustrates the need, on the part of central government, to operationalise measures that protect its information systems. Network
disruptions, unauthorized users, software failures, hardware failures, natural disasters and 
employee errors can prevent information systems from running properly or running at all. The 
government has a National ICT Policy that governs the use of ICTs in Zimbabwe. The issue that 
then arises is whether or not the policy gives direction in terms of addressing ICT risks. There is 
therefore need to analyse the ICT policy to this effect.

Furthermore, the Comptroller and Auditor General’s Report (2013), pointed out that there are a 
number of statutory instruments in place and that these instruments are not being operationalised 
in most of the ministries. For example, the 2013 Auditor General’s Report observed Governance 
weaknesses in internal controls, record keeping and reconciliation of the Sub Paymaster General 
Account with the Public Financial Management System records. Thus the report seems to 
suggest that despite the presence of the Public Financial Management Act (Chapter 22:19), the 
same instrument is not being fully put into practice in almost all ministries. The report further 
notes failure by ministries in complying with statutory procurement regulations. In addition, the 
same report further notes that the issues observed in the current report had also been raised with 
a number of ministries in previous years.

Given that ICT risks are ubiquitous in all system environments, it is important to establish both 
the adequacy and gaps of the ICT risk management policies and strategies that have been 
developed and implemented within the PFMS environment in Zimbabwe.

1.3. Research objectives

The research seeks to achieve the following objectives:

1. To analyse the government ICT Policy that governs the use of ICTs in Zimbabwe in terms of 
its appropriateness in addressing ICT risk management issues within the PFMS environment.

2. To ascertain the current profiles of ICT risk management within the central government’s 
PFMS environment.
3. To determine ICT risk management gaps within the central government’s ICT Risk Management Framework for the PFMS.

1.4. Research questions

The research shall answer the following questions among others:

1) What factors determine successful ICT risk management for Zimbabwe’s Public Financial Management System (PFMS)?
2) What are the current profiles of ICT risk management for the PFMS environment?
3) How are ICT risk management concepts applied within the PFMS environment?
4) What tools can be identified in compiling the ICT risk management framework for the PFMS?
5) How comprehensive are the Service Level Agreements that management signed with its service providers?
6) Has management developed an Internet and security document in consultation with its stakeholders?
7) How often are the reports from the network monitoring tool reviewed and acted upon?
8) Are there any policies and procedures with regard to sanitisation of ICT equipment and media prior to disposal?

1.5. Justification of the study

The concept of ICT risk management, though not so new a phenomenon elsewhere abroad, has not been empirically researched upon in Zimbabwe. There is therefore need to ascertain whether the ICT risk assessment and mitigation initiatives currently in place are comprehensive and at the same time being fully operationalised within the central government’s PFMS environment. The current study seeks to ascertain whether these risk assessments and mitigation initiatives, if they exist, are being carried out on a regular basis. The Comptroller and Auditor General’s Report (2013), pointed out that there are a number of statutory instruments in place and that these
instruments are not being operationalised in most of the ministries. The report seems to suggest that despite the presence of the Public Financial Management Act (Chapter 22:19), the same instrument is not being fully put into practice in almost all ministries. The report further notes failure by ministries in complying with statutory procurement regulations. In addition, the report observed that the Sub Paymaster General Account could not be reconciled with the Public Financial Management System records. This seems to suggest there are system weaknesses that are being exploited in the commission of fraud.

It is therefore against this background, that the researcher feels motivated to explore and establish the adequacy of the ITC risk management initiatives currently in place as well as establishing whether the same are being consistently operationalised, more so with special emphasis within the central government’s PFMS environment.

1.6. Significance of the study

This study seeks to determine the ICT risk management gaps within the central government’s ICT risk management initiatives for the PFMS. The researcher is of the opinion that ICT risk management initiatives within the PFMS environment are either inadequate or are not being put into practical use. Further, the researcher feels that management and operational staff do not fully appreciate the need of implementing adequate ICT risk initiatives despite the failure to reconcile the Sub Paymaster General Account with the Public Financial Management System records, suggesting that the system is being breached. Vulnerabilities cited may then encourage central government as a beneficiary, to take appropriate action in order to safeguard its information systems.

The research findings will also encourage more regular reviews of policies that govern the use of ICTs in Zimbabwe recognising that the ICT sector involves fast changing technologies. The study will also benefit business practitioners who have implemented Enterprise Resource Planning Systems (ERPS) in their institutions but are not operationalising risk management initiatives of their own, basing their risk mitigation strategies on vendor provided security
information. Both government and the business community may also realise the need to practically test the security status of their systems on a regular basis. This study could also serve as an academic tool upon which further research can be undertaken on this subject.

1.7. Assumptions of the research

- It was assumed that the respondents, who by virtue of their positions as managers and technical operatives within the PFMS environment, were knowledgeable about ICT risks and the best practices to manage these risks.

- It was also assumed that the respondents would freely give information with respect to current system weaknesses to the researcher.

1.8. Delimitations of the study

The study was limited to Harare because it is the capital city housing the head offices of all government ministries as well as the head offices of the PFMS partnering companies. The selected population for this study was made up of people who have an ICT technical orientation and are in management and technical operational positions within their ministries, departments or businesses. As such, the study was limited to top level management within the selected ministries and companies because the research is primarily technical in nature. Other possible respondents were deliberately and conveniently left out so as to concentrate on policy formulation and key ICT risk management implementation personnel. The three partnering companies are each responsible for hardware, networking and software respectively.
1.9. Limitations of the study

- The sample respondents may not have been fully representative of the country’s SAP user community in Zimbabwe as it was drawn from only four (4) Government departments and three (3) private companies. To mitigate this limitation, the depth interviews afforded the researcher the opportunity to ask further probing questions.

- There was no ample time to further solicit for senior management authority to conduct record observation in order to ascertain whether system breaches were a result of system weaknesses. Authorisation to access classified information generally takes long to obtain in government.

- Some respondents may have intentionally given false information knowing it to be false. To mitigate this limitation triangulation was used to confirm or disconfirm the information.

1.10. Chapter Summary

ICT risk management policies and strategies that have been developed and implemented within the PFMS environment have to be operationalised and continuously updated. This chapter introduced the research and highlighted the study background as well as study objectives. In chapter two, the research reviews literature in the field of ICT risk management policies and strategies. The next chapter explains both the theoretical and empirical literature surrounding ICT risk management.
CHAPTER II
LITERATURE REVIEW

2.0. Introduction

This chapter provides a theoretical overview of ICT risk management concepts and also serves as a point of departure for the empirical work to be done. The conceptual frameworks will provide working definitions of ICT risk management and related concepts as well as insight into the success factors in ICT risk management, sources of the risk and tools that can be employed to control, mitigate, and avoid the occurrence of risks.

2.1. Overview of risk management

The seminal work to give flesh to the concept of risk management was done by Ulrich Beck’s (1986) Theory of risk society. In collaboration with Giddens and Lash (1994) they elaborated the original work into a more general theory of globalization and modernity and called it Reflexive Modernisation (Beck, Giddens, and Lash 1994). Through the formulation of this theory, Beck and Giddens argue that risk has become a more dominant and characteristic feature of our society at the same time as the nature of risks have changed. They point out that “While nature was the dominant source of old risks (like natural catastrophes), new risks have their origins more in our created environment, that is, our technological and organizational systems”. Therefore, it is this theoretical development that has inspired research on risk related issues in many disciplines.

Hanseth (2007), states that the Theory of the risk society has also more recently been adopted by scholars within Information Systems Studies and cites Ciborra et al. (2000). Hanseth alludes to the fact that, in spite of all research on ICT risks and the increased sophistication of the tools and techniques developed, ICT risks still prevail. The author believes that there are indications that these risks are in fact, increasing rather than diminishing, basing this belief on an observed
growth in ICT complexity, which increases and creates new challenges regarding management and control of the development and use of ICT solutions, coupled with theoretical developments in other areas regarding risk.

There are many Enterprise Risk Management (ERMs) frameworks made available by numerous researchers, but one of the most popular once is the COSO ERM model (2004), which was created by the Committee of Sponsoring Organizations of the Treadway Commission. This framework categorizes risks within the following types: (1) financial, (2) operational, (3) legal/compliance and (4) strategic.

The categorisation of risks also suggests that there are many approaches to measuring operational risk and all differ in terms of quantitative maturity and conceptual rigour. One important scope of the ‘operational’ category of risks deals with risks that are associated with the operations of information communications technology (ICT) (COSO ERM model: 2004). The framework notes that ICTs are nowadays a critical component in all enterprises, forming a layer of the business infrastructure that attracts over half the capital investments of business and thus deserves to be well managed. The framework further notes that ICTs produce diagnostic data that makes tracking, analysing and understanding risk events easier. This encourages getting insights into the causes of risk events and improving their management.

According to Bernstein (1998) risk management started out as an indemnity management purpose. The cost of indemnity had restricted management's alternatives in dealing with the hazards faced by insurance organisations. One of the foremost problems was that insurers rated firms according to business in such a way that fine run firms that had few losses were required to pay for the claims of poorly run firms within the same industry. With this, the role of risk management appeared. Management began to make out that abridged losses projected reduced cost of risk. If risk managers reduced losses they could hold them themselves without resorting to indemnity. However, it took some time for industries to settle in risk management.
The increased interest in risk management is the result of a number of instantaneous drifts. Worth noting is the fact that globalisation of trade and production has augmented financial and direct investment in unstable up and coming markets. Further, risk management has also attracted consideration as a result of the recurring and well publicised breakdowns linked with its execution. Hanseth (2007) points out that regardless of the amplified academic and specialized concentration paid to risk management, common instances still occur when classy investors or firms experience abrupt, unexpected, and devastating losses.

From an economist’s perspective, risk is described as the survival of uncertainty about potential upshots. Risk is a mean reason in economic existence for the reason that individuals and firms create permanent reserves in research and product improvement, inventory, plant and equipment and human capital, without knowing whether the potential cash inflows from these funds will be adequate to pay off both debt and equity holders. If such genuine investments do not stimulate the necessary returns, then the financial claims on these returns will turn down in worth.

In addition to varying the extent of equity and debt in their capital composition, firms/business organisations can also influence their chance of liquidation by justifying the risk disclosures they tolerate. Firms/Business organisations come out to prefer between the types and degrees of disclosures, assuming those that they consider have an aggressive gain in supervision and laying others off into the capital markets (Stulz 1996). Other features of the firm's processes such as the convexity of its tax lists, can also influence the amount to which administrators challenge to alleviate risks (Tufano 1996). Apparently, Besanko, Dranove and Shanley, (1996) believe that economists and strategic planners view risk management as being related to the issue of the confines of the firm. In this structure, the statement to lessen particular risks is comparable to the decision to outsource a particular purpose. Thus, risk management, like technology allocation, or level, is a basis of economical plus.

ICT risk refers to the likelihood that an organisation’s information systems are insufficiently protected against certain kinds of damage or loss (Straub and Welke 1998). This therefore refers to the possible occurrence of an event that has the capacity to lead to loss of or a disruption to an
organization’s operations, services, or functions which, if not managed, can escalate into an emergency, crisis, or disaster. The literature on ICT risk management indicates that risks increase with the increased adoption of ICT in business. This seems to suggest that there is need to budget adequately for the implementation of ICT risk management within the PFMS environment. The current research will therefore want to establish whether adequate funding is being made yearly so as to enable the ministry address issues pertaining to successful ICT risk management.

In order to deal with system risks, Straub and Welke (1996; 1998) note that risk can be reduced or managed only when managers are aware of the full range of IT risk management controls available and are able to pick and implement the most effective among the available controls. They developed a theory based information security program and used it to deal with system risks in two Fortune 500 firms. The theory included use of a security planning model, education and training in security awareness and use of a countermeasures analysis matrix. The security planning model is as illustrated below.

**Managerial perceptions of security risk**

![Figure 1: Model for Managerial Perceptions of Security Risk](image)

*Adapted from Goodhue and Straub (1991)*
Using the model above, the researchers argue that managerial concern about organisational security is therefore a function of risks inherent in the industry, the extent of the effort taken to control these risks and the individual factors such as awareness of previous system breaches and perpetrator background knowledge in systems work. They further note that managers should therefore be well informed about incidences of computer abuse and susceptibility to damage hence they should take preventive action such as use of passwords. Straub and Welke also indicate that there is need to educate and train staff on issues pertaining to ICT systems risks. Likewise, the current research intents to analyse the management plans so as to establish whether management is aware of the risks inherent within the PFMS environment and the actions that they have put in place in order to deal with risks emanating from employee behaviours in the work place.

According to Straub and Welke (1996), countermeasures to reduce risks fall in the categories of deterrence, prevention, detection and recovery. The general deterrence theory suggests that “active and visible policing is thought to lower computer abuse by convincing potential abusers that there is too high a certainty of getting caught and being punished severely”. Preventive measures refer to actions such as locking computer room doors and use of password access controls. Detection will be concerned with the organisation having the capacity to detect misuse. Thus it will entail system audits and virus scanning so as to gather evidence of misuse and to identify offenders. Recovery, as a security program will address issues with regard to correcting the harmful effects of abusive acts, although this will not assist in deterring future computer abuse. However, Straub and Welke concede that “there is limited evidence in practice for the effectiveness of these techniques despite the strong theoretical basis,” (Straub 1990).

In the Straub and Welke study, interviews were held with top management in the two firms over a period of fifteen (15) months as part of their empirical study to support their theory. They concluded that no system can be made absolutely secure from risks. They therefore recommended that those parts of the security plan that can be formalised should be so formalised in order to free resources for use in monitoring those areas of security that cannot be formalised.
Badenhorst (1994) also undertook research with the objective of developing a formal theoretical model to address IT risks and optimising the process of ICT risk management within organisations. He notes that in an ideal ICT risk management model, all aspects of a risk management process should be covered. This would include risk identification, risk analysis, risk assessment and finding the optimum resolution for a specific risk context. Figure 2 below illustrates the issues and elements that need to be fully addressed for successful ICT risk management.

**Framework for ICT risk management**

<table>
<thead>
<tr>
<th>Domain of ICT Risk management</th>
<th>ICT completeness</th>
<th>IS Security completeness</th>
<th>Risk approach completeness</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Organisation</td>
<td>• Information security.</td>
<td>• Risk identification</td>
</tr>
<tr>
<td></td>
<td>• Personnel</td>
<td>• Technological</td>
<td>• Risk analysis</td>
</tr>
<tr>
<td></td>
<td>• Documentation</td>
<td>information security.</td>
<td>• Risk assessment</td>
</tr>
<tr>
<td></td>
<td>• Software</td>
<td>• Application</td>
<td>• Risk resolution</td>
</tr>
<tr>
<td></td>
<td>• Data</td>
<td>information security.</td>
<td>• Risk monitoring</td>
</tr>
<tr>
<td></td>
<td>• Networks and</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Hardware</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Environment</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Figure 2.1: Badenhorst’s framework for ICT risk management.*
Badenhorst (1994) notes that any ICT risk management initiative should, “in a dynamic and comprehensive way, address the entire information communication technology field as far as possible”. For example, the organisational structure should be conducive for the implementation of the ICT risk management initiatives. For the current study, this would suggest having the right personnel who can fully document all the organisation’s systems and are able to use and develop the current software so as to maintain data integrity and confidentiality. The networks and the hardware should also be correctly configured and be readily available to authorised staff as alluded to by Kumsuprom (2010). These should also be appropriately protected from both internal and external environmental threats. Such initiatives would further suggest proper management of access rights and the installation of firewalls. Badenhorst (1994) further suggests that there should be appropriate policies and procedures to guide staff in order to attain information security completeness. Thus he seems to indicate the presence of a risk statement for the organisation as a whole. The risk statement would then serve to direct staff in the formulation of clear risk management objectives and risk boundaries so as to fully address issues of risk identification, analysis, assessment, resolution and monitoring. Thus it is pertinent that the current research adopts this strategy when trying to establish the existence of policies to deal with ICT risks within the PFMS environment.

Within the information security realm, risk is defined as the probability that a threat agent (cause) will exploit a system vulnerability (weakness) to create a loss to the confidentiality, integrity and availability of an asset (Carroll, 1996). Therefore various events or incidents that compromise IT in some way can cause adverse impacts on the organization’s business processes or mission. These events may range from being merely inconsequential to catastrophic in scale. Assessing the probability of likelihood of various types of events or incidents with their predicted impacts or consequences, should they occur, is a common way to assess and measure IT risks (ISO/IEC 17799: 2005). Alternative methods of measuring IT risk typically involve assessing other contributory factors such as the threats, vulnerabilities, exposures, and asset values. There are also many Enterprise Risk Management (ERMs) frameworks made available by numerous researchers, but one of the most popular once is the Committee of Sponsoring Organizations (COSO) ERM model, which was created by the Treadway Commission. This
framework categorizes risks within the following types: (1) financial, (2) operational, (3) legal/compliance and (4) strategic.

Much research has been undertaken with regard to finding out the best practices to deal with ICT risk management within organisations. Worthy of note is the research by Solms (2005b), who concludes that, integrating control processes of the COBIT framework and the ISO/IEC 17799 standard work best through a two-way approach to ICT risk management. The author states that, “the COBIT framework lays the foundation of a top-down approach to risk management, while the ISO/IEC 17799 standard supports a bottom up approach. He observed that three success factors to deal with ICT risk management were:

- Creating organisational policy (drawn from both the COBIT framework and the ISO/IEC 17799 standard),
- Managing reliable ICT resources (drawn from the COBIT framework), and
- Effectively planning enterprise information security (drawn from both the COBIT framework and the ISO/IEC17799 standard).

While the theoretical literature review authors so far cited in this research seem to agree on the definition of ICT risk, its possible sources and possible ways of managing the risk, it is crucial to realise that none, except for Solms (2005) mention the need for an organisational policy document. Ordinarily, this is the document from which the organisational strategic direction will be formulated. Further, it is from the same policy document that an organisational risk statement and the risk management methodologies for the management ICT risk management plan will be formulated. The risk statement and the risk management methodologies will then appear in the operational level plans as action plans for use in attaining successful ICT risk management for the organisation as a whole (Kumsuprom 2008). The research findings further emphasise the need to analyse the government ICT Policy that governs the use of ICTs in Zimbabwe in terms of its appropriateness in addressing ICT risk management issues within the PFMS environment.
2.2. Success factors in ICT risk management

Theoretical research findings by Solms (2005) were empirically confirmed by Kumsuprom et. al (2008) who carried out a research to validate the nature of the success factors in ICT risk management in three Thai businesses. The researcher compared ICT risk management practices in those firms with the COBIT framework and the ISO/IEC17799 standard. The objective was to come up with a single management framework to address operational, technical and strategic risks related to ICT use. The study also concluded that the development of organisational structure, organisational process, organisational control and organisational ICT strategies, were essential in successfully dealing with ICT risk management.

Closely related to the above, is a case of a regional US Family Grocery (FG) chain in which the Info–Tech Research Group undertook risk assessment management using COBIT 5 as the guide. In that study, the FG Board requested its IT department to formally manage IT related risk. The mandate specifically called for an initial high level assessment of IT organisational risk, drawing largely from internal expertise. The board also requested that the IT department demonstrate an ongoing program to manage risk. A workshop to this effect was undertaken with Info-Tech Research Group as facilitators. Info-Tech based the workshop on COBIT 5 because of COBIT 5’s clear and concise framework for capturing key ICT processes.

The proceedings of the workshop noted that the FG Information Technology department had no functioning ICT risk management processes in place. The ICT department leveraged the Info-Tech facilitator and methodology to conduct high level team brainstorming with key team members, aimed at identifying ICT risk factors relevant to the client organization. The team then documented risk events, identifying actors and threat types. A prioritisation rubric was developed and applied to sort the risk events. The team documented (where programs were in progress) or identified (net-new programs) the resources/time needed to mitigate the priority risk factors. Finally, the team made critical decisions to determine the shape of the ICT department’s ongoing risk management. These included definitions of roles and responsibilities, management activities, information gathering activities, and communication plans.
As the decisions were achieved, each was codified in the relevant program manuals, standard operating procedures, assessment tools, project requests, and templates for policies and communication. The key outputs from this workshop included:

- A catalogue of IT risk events which not only documented risk events but also the high-level mitigation strategies, initiating IT project requests as needed for items not already on their project calendar.

- An IT risk management program guide, which captured critical decisions, including the team’s rubrics for assessing risk event severity and risk event likelihood. The document described the ongoing IT risk management steering committee process to which the team committed during the workshop.

- A presentation to the firm’s board on the IT risk management assessment and program. This presentation described the progress made during the workshop, highlighted key risk factors and remediation, requested additional budget, and summarised the ongoing risk management program to the board.

The US Family Grocery (FG) case study by the Info–Tech Research Group and the Kumsuprom et. al (2008) case studies indicate that there are generic aspects that must be in an ICT policy for it to be effective in terms of successful ICT risk management. These are the development of organisational structure, organisational process, organisational control and organisational ICT strategies. In the current study, the researcher will need to assess whether these aspects are also being addressed by the current National ICT Policy and hence gaps will be identified.

2.3. Identification of sources of ICT risk

McEvoy and Whitcombe (2002), among many, are researchers who undertook studies to identify the sources of ICT risks in organisations. They conclude that risk elements are related to either ICT use or to IS management. They state that ICT risk emerge from poor ICT risk management
processes in various departments. For example, ICT risk resulted from uncontrolled practices including the use of pirated applications and software, improper or incomplete software licensing, poor protection of intellectual property and from incomplete software maintenance and updating. On the other hand, the authors note that IS risk result from poorly managed or constructed databases, poorly managed servers, old operating systems, poor networking management and maintenance, poor setting of configurations and penetration testing breaches. They also noted that in order to manage risks, each organisation had to define the appropriate control mechanisms for management of existing ICT resources and information security, based on its complete understanding of people, processes, technology and systems.

These research findings by McEvoy and Whitcombe (2002) were further confirmed in the research by Kumsuprom et.al (2008). The later research also revealed that in order to manage risks, each organisation should define the appropriate control mechanisms for management of existing ICT resources and information security, based on its complete understanding of people, processes, technology and systems in the organisation. The respondents in the Kamsuprom Thai case studies said that their objective was to control the processes, technology and systems appropriately by delegating the responsibilities to people within their organisations in order to achieve business objectives and goals. The Thai organization’s objectives focused on security issues by developing a systematic process to protect organisational technology and systems from a variety of problems related to operational, strategic and technical risks of corporate data loss, or business continuity. To achieve this, all the organisations in the study noted that ICT and IS objectives were best addressed by adoption of and clarity in various organisational policies. This supports earlier research findings by Smith and Eloff (2002), who suggest that when dealing with ICT risk management, policies to direct information technology and information security need to be defined separately as this enables the setting of information technology objectives into the information technology policy and the setting of information security objectives into the information security policy so as to successfully deal with ICT risk management in the organisation.
The findings from the study by McEvoy and Whitcombe (2002) indicate that ICT and IS risks can be effectively prevented or mitigated within organisations through appropriately structured management plans. In the current research, there will be therefore need to analyse and establish whether the management plans in place give appropriate direction toward attaining successful ICT risk management within the PFMS environment.

In their study of the Thai business organisations, Kumsuprom et.al (2008) observed that the respondents identified an organisational policy as the enabling document in risk definition, the setting of responsibilities for risk management at all management levels, outlining the risk management methodology and determining and making explicit risk control and auditable areas statements. The policy statement (i.e. a risk statement) in the Thai interviews was most often derived from their adoption of either or both the COBIT framework and the ISO/IEC 17799 standard. Hence the practice was in compliance with the COBIT framework which states that an organisational policy document must exist to enable successful ICT risk management and provide the general and specific responsibilities for ICT risk management so as to align IT with the organisation’s business (ITGI 2007; ISO/IEC 17799: 2005). The same research also concluded that the organisational policies needed to be communicated to staff and that it was essential that staff roles and responsibilities were also clear when risks occurred. The Kumsuprom et.al (2008) research also concluded that business continuity planning was a key element of organisational policy in each company. Thus the business continuity plans served as contingency plans for successfully dealing with strategic, operational and technical risks in the organisations. In addition, incorporating business continuity plans in the organisational policy would positively affect planning at both the corporate level and the operational level when undertaking ICT risk management.

The use of standards seems to facilitate the implementation of appropriate risk management policies within organisations. It will be pertinent that in the current research, the relationship between the policies and standards in place be established as well. The policy statements should be traceable to the standards in order to attain successful ICT risk management within the PFMS environment.
Creating both an ICT policy and an information security policy were confirmed in the survey analysis as being key indicators of success in ICT risk management. Both ICT and IS policies were shown to be significant indicators since their clarity gives clear directions essential in defining and then managing ICT risks at the senior management level. Furthermore, the organisational policy enabled the organisations to clarify both their ICT and IS objectives. The policy document also covered both the management of ICT resources and the management of information security simultaneously. The policy document was further used to outline brief risk definitions, the responsibilities for risk management, risk management methodology, risk control and auditable areas. The focus of the organisational policy document was to ensure that ICT risk management was clear at all staff levels in order to perform organisational planning appropriately at both the corporate and the operational levels in ways similar to that prescribed in the ISO/IEC 17799: 2005).

According to Kumsuprom et.al (2008), organisational policy required senior management to generate both the ICT and IS policies in order to achieve successful ICT risk management. The statistical results in their research revealed that organisational policy was a significant factor for successful ICT risk management. Creation of the organisational policy at the senior management level required the operational managers to control ICT resources and to plan enterprise information security in order to achieve successful ICT risk management.

McEvoy and Whitcombe (2002), Smith and Eloff (2002) and Kumsuprom et al (2008) all seem to be in agreement with regard to the elements that constitute both ICT and IS risks. However, only Smith and Eloff (2002) and Kumsuprom et al (2008) go further to elaborate on the remedial actions essential in attaining successful ICT risk management. While the former is silent on the issues of ICT policy clarity, assignment of risk management responsibilities including staff roles and responsibilities and communication of the same to staff at all levels, the later authors elaborate and emphasise that ICT and IS policies should be separately defined. However, only Kumsuprom et al (2008) make reference to the use of ICT risk management frameworks (COBIT) and standards (ISO/IEC 17799:2005) in considering success factors and the current profiles of ICT risk management within organisations.
2.4. Applying ICT risk management concepts

Luftman et al. (1993); O’Brien and Marakas (2006); Smith and Eloff (2002); and Whitman and Mattord (2009), as cited in Kumsuprom (2010), note that the implementation of control mechanisms to maintain data and information integrity are essential as this also affect control planning at both the corporate and operational levels. They further note that use of ICT controls and audit plans aid organisations to identify and maintain reliable ICT infrastructure. In addition, managing proper licensing and proprietary of ICT resources were also noted as necessary for successful ICT risk management. This included secure management of facilities, networking, personal computers, database management systems and software.

In the Thai study cases, ICT control and audit plans were used to identify and maintain reliable ICT infrastructure. Maintaining reliable ICT infrastructure included having sufficient networking connections, having efficient database systems, and providing proper or complete software and applications licenses. The respondents believed that management of reliable ICT resources directly affected successful ICT risk management, confirming the findings from previous research by Luftman et al. (1993); McLeod and Schell (2007); McNurlin and Sprague (2002); O’Brien and Marakas (2006); and Whitman and Mattord (2009) as cited by Kumsuprom et. al (2010), which showed that management of reliable ICT resources enabled organisations to prevent, avoid and mitigate operational risks.

The respondents in the case studies also argued that database systems management affected maintaining of data and information integrity. They further indicated that database systems management was essential for the proper and effective management of ICT resources, and this therefore had an influence on successful ICT risk management. They based this argument on the understanding that operational risks related to ICT can be mitigated, avoided and prevented by the adoption of such initiatives. The findings from the previous research of Straub and Welke (1998) had showed that managing database systems helped organisations maintain data and information integrity to achieve the effective management of ICT resources. The indicator, “managing database systems”, was then confirmed as having an impact on the effective
management of ICT resources in the survey analysis. The reason given by the interviewees was that database systems management enabled maintaining data and information integrity while effectively managing ICT resources to achieve successful ICT risk management.

Establishing data and information integrity as well as proper management of ICT resources are an integral part of the current research on ICT risk management within central government’s PFMS environment. To this end, the researcher will again seek to establish whether the database management policies in place are being fully operationalised. Thus the researcher will need to establish the existence of management ICT controls and audit plans.

Providing proper or complete software licensing was also of concern among the respondents as they believed that it had an important influence on their effective management of ICT resources. They noted that software piracy caused obstruction of their commercial license agreements and this led to operational risk thereby directly affecting successful ICT risk management in their organisations. Risk management in the Thai organisations related not only to software used in the organisation but also to software installed on the personal computers of staff, both of which impacted on the ICT operations in their organisations. Lloyds (2000) argued in previous research that all intellectual property must be used under property rights. In addition, Rife (1994) mentioned that software piracy is the single greatest threat to the continued success of the industry. Rife further added that the piracy rate in Thailand was estimated to be 99%+. Thus Thai businesses have now started to become more concerned about software licensing. Since 2007 the Royal Thai Government has passed a new law on computer related offences, the Computer Crimes Act, which all Thai business organisations are forced to follow.

The Kumsuprom et al (2008) Thai case studies highlighted the importance of managing software licensing as integral to ICT risk management. Providing proper or complete software licensing was therefore confirmed as a determinant of effective management of ICT resources. The reason given by the interviewees was that providing proper or complete software licensing enabled their organisations to avoid operational risk emerging from software piracy. The effective management of ICT resources in the Thai businesses studied required providing sufficient
networking connection, effectively managing database systems and providing proper or complete software licensing to achieve successful ICT risk management.

The statistical analysis results in the Thai case studies showed that the management of ICT resources was a significant factor for successful ICT risk management. The research also showed that the relationships between the effective management of ICT resources and effective planning of enterprise information security were significant to establish successful ICT risk management. The adoption and implementation of the effective management of ICT resources was shown then to also be a factor in ICT risk management success in Thai business organisations.

The Kumsuprom et. al (2008) case studies noted that software licensing enables the client organisation to be periodically receiving system updates from the vendor organisation. The research further notes that software licensing enables the client organisation through upgrades, to incorporate new system functionalities within its systems as well as providing the client organisation with enhanced weaponry to deal with new system bugs. Licensing fees are also in conformity with the due respect to be bestowed on intellectual property rights. The researcher will therefore need to establish whether licensing is being effectively observed to enable the ministry attain successful ICT risk management within the PFMS environment.

Rife (1994) and Lloyds (2000) as cited in Kumsuprom (2010) and Straub and Welke (1998), all discuss the essentials of maintaining both data and information integrity from different dimensions. However, these dimensions seem to fall under two classes of namely proper database management and respect to the issue of intellectual property rights. Thereafter, issues of control mechanisms such as system access rights, use of audit plans, ownership of ICT resources and licensing can then be elaborated upon. A synthesis matrix on the application of ICT risk management concepts to maintain data and information integrity within organisations seem to suggest that discussions on this subtopic get more elaborate depending on the time the study was undertaken. For example, Rife (1994) as cited in Kumsuprom (2010) seem to have dwelt on the issues of software piracy and respect for intellectual property rights to include licensing. On the other hand, Kumsuprom (2010) discusses the same issue under more elaborate subheadings of
ICT risk management controls, use of audit plans, licensing, database management and ownership of ICT resources.

2.5. Tools that can be identified in compiling the ICT risk management framework

The US Family Grocery (FG) case study by the Info–Tech Research Group and the Kumsuprom et. al. (2008) case studies indicate that there are many tools that can be identified in compiling ICT risk management frameworks for different organisations. These among many, would include an ICT Governance Policy, Management of Information Technology Security (MITS) Procedures documents, Management ICT risk management plans and Operational ICT risk management plans and procedures.

2.5.1. ICT Governance policy

In the three Thai organisations case study, (Kumsuprom et al. 2008) the third factor that emerged as having an impact on ICT risk management related to the various components of the enterprise information security plan. Consistent management and planning of people and their behaviour in an organisation (the control mechanisms of implementing organisational information security), and the development of both corporate and operational plans, were all shown to, in combination, impact on ICT risk management. The interviewees argued that the effective management of staff and their behaviour in organisations included four areas of focus namely; defining the responsibility of employees, securing information security with regard to employees’ behaviour in the organisation, protecting information security with regard to employees’ behaviour in the organisation, and providing training and education programs for staff.

Effective segregation of duties is all about clearly defining employee roles and responsibilities and ensuring that these do not overlap. Thus accountability for possible system breaches will be associated with a specific individual. Operational plans should therefore be able to address such issues; hence the current research will seek to establish whether employee roles and...
responsibilities are clearly defined within the PFMS environment toward the goal of successful ICT risk management.

By addressing all four areas, they believed that operational risk related to ICT could be mitigated, avoided and prevented, in order to achieve successful ICT risk management. The respondents in the case studies noted that the effective management of people in the organisation affected the planning of control responsibilities of employees at both the corporate and the operational levels in ICT risk management. It was also clear that the planning of control responsibilities of employees at the corporate level was used to balance the bottom-up control aspects developed at the operational level. Senior management at the corporate level set up committees to take responsibility for addressing all identified risks (e.g. business risks, ICT risks and IS risks). On the other hand and in addition, managers at the operational level established practices for the operational team to account for specific risks (e.g. operational, technical and strategic risks). They then reported the results back to the committees in order to obtain a review and gain advice from the committees for further treatment of particular risks.

The respondents in the Thai case studies argued that the control responsibilities of employees were evident in three specific areas, that is, business, technological and security directions and each had to be addressed to deal with operational risks. The control responsibilities of employees were previously discussed in researches by Straub and Welke (1998), who argued that the role of staff members (e.g. the board and all management levels) was to define how to achieve the objectives of risk management. The objectives in the Straub and Welke (1998), study included prevention, mitigation and avoidance of operational risks in ICT risk management. Defining clear roles and responsibility of people in organisations, they believed, directly influenced the effective management of staff and their behaviour in achieving successful ICT risk management. The implementation of information security policies with regard to the behaviour of staff in organisations, as revealed by the respondents in the Straub and Welke (1998) study, was required to effectively manage people and their behaviour in organisations.

Previous research by Smith and Eloff (2002) had identified that the safety of information related to its confidentiality, complying with organisational security rules and regulations. The study
concluded that it was therefore necessary to regularly check ICT facilities to ensure maintenance of security implementation standards and to regularly review the effective planning of enterprise security to ensure compliance with organisational security policy and standards. Complying with security rules and regulations in the organisations and other external regulators were shown to be significant and as being supported by the adoption of the ISO/IEC 17799 standard which elaborated the details of security compliance (ISO/IEC 2005). In addition, national regulations and laws generated by external regulators such as the Stock Exchange of Thailand (SET), the Security Exchange of Thailand (SEC), the Bank of Thailand (BOT) and the Royal Thai Government, were also considered in each organisation in order to help the Thai businesses prevent and avoid the operational, strategic and technical risks related to ICT risk management.

While people are every firm’s most valuable asset, it is critical to note that their behaviour in the work environment is aligned to the attainment of organisational goals and objectives. Thus for the current research, there will be need to ascertain how management plans affect both human resources management planning and ICT information security as well as IS security. A management statement to this effect will therefore assist the researcher to fully address the research questions.

Protecting data and privacy was the last element identified in that research as critical to the effective planning of enterprise security when dealing with ICT risk management successfully. Data protection and privacy involved the monitoring process that maintained data protection and privacy. The significance of protecting data and privacy for the Thai organisations corresponds with similar conclusions in research by Hughes (2006b); Hilton (2009) and Martinez et al. (2010), who each suggested that data protection and privacy must be implemented in order to facilitate advances in risk management technology. The Kumsuprom research therefore proposed that the effective planning of enterprise information security is a key success factor for planning ICT risk management. In the Kumsuprom research, the respondents indicated that securing information was used to prevent and protect organisational assets which include information, information technology and systems. Securing organisational information in relation to employee behaviour was shown in the case studies to be related to the control of the level of personnel
access, or to the access rights of employees to information (e.g. specified information related to staff’s job descriptions), to information technology (e.g. specified software and applications related to staff’s job descriptions) and to systems (e.g. a specified module related to staff’s job descriptions).

Furthermore, the respondents in the case studies revealed that securing information security in employee behaviour was mostly concerned with the control process governing employees during employment (e.g. training and educating program), at termination of employment (e.g. transferring to new position and quitting the position) and at change of employment (e.g. transferring to new position). Securing information in the organisation from employee behaviour, they believed, directly influenced the effective management of people and their behaviour in the organisations.

The protection and security of information with regard to employee behaviour (i.e. an insider threat) was revealed in the case studies as influencing the effective management of people and their behaviour in the organisations. The respondents argued that protection was best assured through employment agreements. They further explained that new staffs were required to understand organisational regulations, rules and about access to confidential information prior to employment (i.e. through orientation programs as well as training and educating programs). Protecting information from inappropriate employee behaviour was, they revealed, a control process to prevent operational risks occurring as a result of human abuse and/or error, whether or not intentional.

In addition, employment agreements were used in the Thai business organisations to prevent the disclosure of sensitive organisational information. The Thai business organisations identified that they followed either or both the ISO/IEC 17799 standard and the COBIT framework in order to manage operational risk in achieving successful ICT risk management. The business organisations considered that protecting information security when employing new staff was achieved by induction of all new employees following the standards in use (ISO/IEC2005; ITGI 2007). Training and education programs were used for the effective management of employees.
and their behaviour in each of the case study organisations. These programs were used to raise awareness of ICT and IS security among employees.

The current research will also seek to establish whether induction programs for new recruits and refresher or enhancement courses for serving employees are being regularly conducted within the PFMS operating environment so as to increase employee awareness in terms of both ICT and IS security. The current study will therefore further seek to establish the existence of signed forms as evidence that both ICT and IS security policies, rules, regulations and procedures are being communicated to the employees.

Interviewees with staff in the Thai business case studies demonstrated that a training and education program was an imperative process to improve the understanding of staff about both ICT and ICT security risks. For example, organisational e-learning was introduced in one case study to inform employees in the organisation about the procedures related to staff producing organisational information in a secure way and the potential disasters, such as installed pirated software, that can result from ICT abuses and misuse of ICT. Training and education programs were also raised with new employees to inform them of all organisational rules and regulations, and were also raised with current employees in order to prevent operational risk related to the use or misuse of ICT. The abuses and instances of misuse of ICT were identified by the interviewees as including playing games online (e.g. a cause of computer viruses) and installing pirated software (e.g. direct effect on operational risk). In the Thai organisations ICT abuses and misuse of ICT were monitored and controlled by the operational manager in each department. In addition, the findings from Straub and Welke (1998) showed that human resources must be trained and educated in order to gain a thorough understanding of organisational vulnerabilities and of the resources required to secure organisational information and systems. In all of the Thai case studies, the ISO/IEC 17799 standard was the framework used to manage human resources.

Sources of both ICT and IS risks seem to be inherent in employee activities within the work environment. It therefore becomes pertinent that the researcher establishes the effectiveness of employee activity monitoring tools within the PFMS environment. There will also be need to
establish the type and frequency of training courses that is being given to employees so as to increase their ICT and IS security risk awareness.

The ISO/IEC 17799 standard enabled the Thai business organisations to define training and educational programs for both new and serving staff to ensure that all employees of the organisation received appropriate information security awareness training. These programs also served as evidence that information security and awareness training were being formally communicated to staff within the organisations. The programs therefore focused on employee controlling roles and responsibilities, securing and protecting information security regarding staff behaviour, and providing training and educating programs to prevent, avoid, and mitigate operational risk. Previous research by Willcocks et al (2006) also indicated that the skills and abilities of human resources contribute in enabling the organisation boost its business performance and in successfully dealing with operational ICT risk management.

2.5.2. Management of Information Technology Security Procedures

Management Information Technology Security (MITS), Procedures assist organisations to maintain both data and information integrity. As alluded to by Kumsupron et. al (2010) crafting the procedures involve identifying the control mechanisms necessary for protecting and securing both data and information integrity. The author therefore concluded that the procedures need to address issues dealing with the proper setting of system configurations, defining access control policy, managing data and information integrity, complying with security rules and regulations, both internal and external, protecting data and privacy, and protecting the physical environment. The respondents in that case study believed that those determinations positively influenced the effective management of organisational information security to mitigate, prevent and avoid technical or security risks in successful ICT risk management. The respondents further argued that the setting of system configurations was required to effectively manage information security and achieve successful ICT risk management.
The success of ICT and IS risk management initiatives put in place in any organisation seems to depend on the plans that the management and operational levels have put in place so as to attain successful ICT and IS risk management. The current research will therefore seek to establish the appropriateness of these plans in dealing with both ICT and IS risks successfully. Thus the research will have to establish the appropriateness of systems, networks and software configurations within the PFMS environment.

In the Kumsuprom et al (2008) Thai case studies, configuration setting was undertaken in operating systems (e.g. Windows server, Linux and UNIX), in networking operating systems (e.g. Netware and Cisco), in business software (e.g. SAP and business solution software) and in hardware systems and operations (A/S 400, Hubs, Switches and Routers). The case study interviewees believed that information security operations that caused technical risk were prevented, avoided and mitigated because a malfunction of ICT or systems in which configurations were properly set could not occur.

The Thai business organisations in the Kumsuprom et al (2008) case studies adopted both the ISO/IEC 17799 standard and the COBIT framework to deal with the issue because they provided frameworks, either at the senior management or operational levels, to enable them to institute processes for managing technical or security risk associated with the use of ICT (ISO/IEC 2005; ITGI 2007). The respondents revealed that another control mechanism for the effective management of organisational information security was development and implementation of an access control policy. The access control policy was focused on the level of access rights to network systems and personal computers. Each of the organisations revealed that there was need for official documentation of the access control policy and that it was essential to maintain and review access control rights on a regular basis. The official access control policy included defining only authorised persons to have access to network services, using both user allocation and password management systems, limiting the level of access to computers and systems as well as monitoring access of log files to prevent unauthorised access. In the case studies, logical access controls were used to protect and secure sensitive organisational assets such as raw data, information, information technology and systems.
According to the SAP Business Objectives Governance, Risk and Compliance (GRC 10.0) standards, granting of excessive system access rights to employees has been noted as being responsible for most of the fraudulent cases reported and qualifying audit reports in most organisations. The current study will therefore need to establish whether system access rights are being managed appropriately. The research will therefore further seek to establish the consistence with which the ICT and IS security policies are being applied within the PFMS environment.

In addition, the Thai business organisations businesses adopted both the ISO/IEC 17799 standard and the COBIT framework to enable the effectiveness of the access control policy (ISO/IEC 2005; ITGI 2007). The respondents in the case studies revealed that management of data and information integrity was important because these organisations were using information security to monitor and secure the processes of producing data (i.e. input process), storing data (i.e. processing process) and disseminating information (i.e. output process). Smith and Eloff (2002); and Solms (2005); ISO/IEC (2005); ITGI (2007) had previously shown in their researches that maintaining data and information integrity were important in the organisation when dealing with technical or security risks.

The respondents in the Thai organisations noted that validation check applications were used to maintain data and information integrity. Validation check applications were used to validate data appropriateness before putting data into applications and systems, to detect any corruption of information through processing errors and deliberate acts and to validate output data from applications systems for its correctness and appropriateness before being distributed. These processes were controlled and monitored in the Thai organisations to ensure that their data and information had integrity. For example, one organisation adopted penetration tests and security scanning tools to monitor and control all organisational transactions in order to ensure that all business transactions were performed properly and correctly.

These methodologies are pertinent to the current research and will assist the researcher to validate whether such policies, regulations and procedures do prevail and are being
operationalised within the PFMS environment. The same methodologies will also help in the identification of ICT risk management gaps within the PFMS environment.

Data protection and privacy were other elements of the effective management of organisational information security. Anderson and Choobineh (2008), and Księżopolski and Kotulski (2007) as cited in Kumsprrom (2010) had previously shown in their researches that protection of information assets on every staff level in organisations must be secured. Data protection and privacy for the Thai organisations related to the protection from both external and internal threats to personal privacy such as malware, viruses, and worms from staff email and personal files (e.g. songs, movies and animated pictures) brought in from outside the organisation. The internal threats problem, they noted, could be controlled, by using software scanning tools that automatically detected threats posed by staff misuse. For example, pirated software installed on personal computers in the organisation could be detected, after which software scanning tools would automatically remove unwanted software from the computers in order to prevent, protect against and avoid any harm related to technical or security risks. Only one of the Thai organisations took action to include this in their ICT risk management processes.

Software scanning tools assist an organisation in dealing with both ICT and IS risks that emanate from inappropriate employee behaviour within the system environment. The use of these tools is also relevant to the current study. The current study will therefore seek to establish the presence of such tools within the PFMS environment.

Security compliance was another critical element in the effective management of information security that emerged from the case studies, in part as a result of the Royal Thai Government having enacted the Computer Crime Act regarding computer abuse (AHRC 2007). McEvoy and Whitcombe (2002) had argued that security compliance entailed clarifying the details of organisational information security. Organisational information security covered prevention, mitigation and avoidance of threats, and vulnerability of organisational assets including internal and external impacts. Moreover, organisational rules and regulations were also involved because the respondents in the case studies argued that their organisations needed to ensure that all ICT
and ICT security procedures and processes were performed appropriately and correctly. The respondents revealed that ensuring security compliance was elaborated in their ICT risk management process and to do this they adopted the ISO/IEC 17799 standard (ISO/IEC2005) and part of the COBIT framework (ITGI 2007). The setting of system configuration, managing and documenting access control policy, managing data and information integrity, protecting both data and privacy and regularly reviewing and updating security compliance were required to effectively manage organisational information security.

The continued emphasis on the use of standards, policies and procedures suggest that these tools can assist an organisation successfully deal with ICT and IS risk issues within organisations. Such a methodology will also assist in the current study as the researcher seeks to establish the level of awareness and preparedness that management has implemented within the PFMS environment in order to successfully deal with both ICT and IS risks within the PFMS environment.

2.5.3. Management ICT risk management plans

ICT risk management was always planned at the corporate level in the Thai organisations. A corporate plan represented the procedures used for ICT risk management as the overall plan for the organisation. The top-down approach and the bottom-up approach can help the organisation strengthen the effectiveness and efficiency of its plan at both the corporate level and the operational level as alluded to by Solms (2005b).

To strengthen effectiveness of a plan at the corporate level, the respondents in the Thai case studies argued that ICT risk management planning was essential as it would be used in setting up the process for the treatment of ICT risk problems in the operational level plan. The value of the corporate level plan was also supported by Martin (2003:3) who described how an organisation adopted a management perspective that seeks to identify the integrated set of broad factors, both strategic and operational, that influence the current practice of configuring the architecture, resources and methodology elements in organisational ICT risk management. The respondents in
the Thai organisations revealed that the effectiveness of a corporate plan included defining the
details of ICT processes, the details of ICT control and audit plan and classification of
information technology for dealing with ICT risk management successfully.

ICT control and audit plans were also identified as important in the case studies, as helping the
organisation to provide the guidelines for ICT control, particularly with regard to ICT processes
included in the corporate plan. The respondents saw the ICT control and audit plan as directly
influencing the effectiveness of a corporate plan in achieving successful ICT risk management.
ICT control and audit covered technological functions that fitted organisational policies. A
corporate plan was also considered in the COBIT framework. This framework explicitly showed
that the aim of ICT control at the corporate level is to achieve effective ICT management of the
risk in business processes (ITGI 2007). In addition, assessing and managing ICT risks in the
COBIT framework were the preliminary focus to plan a brief overview of ICT applications
control and ICT security control. Solms (2005a) suggested that the COBIT framework also
helped the organisation develop guidelines for ICT risk management at the senior management
level by providing a framework for control processes.

Corporate level plans, management and operational level plans, in conjunction with the use of
standards, are again being cited in an organisation’s effort to attain successful ICT risk
management within the firm environment. This seems to suggest that for the current study, the
researcher needs to establish the rapport between the National ICT Policy and the ministry’s
management and operational level plans. The existence of a top-down approach and a bottom-up
approach among these plans will assist the ministry to successfully deal with ICT risks within the
PFMS environment (Solms 2005b).

Classification of ICT resources in ICT risk management was also considered as important by the
respondents in the Thai case studies because ICT applications and ICT security were distinct
from each other. This determination was seen as directly affecting the effectiveness of a
corporate plan when dealing with successful ICT risk management. It helped the businesses to
distinguish the difference between the degree of control of ICT itself and control of ICT security.
Therefore, identifying the scope of ICT applications and ICT security needs, at the corporate level through a corporate plan, provided an overview of the appropriate treatment of ICT and ICT security in the organisation. This classification of ICT is also a key element in both the COBIT framework and the ISO/IEC 17799 standard (ITGI 2007; ISO/IEC 2005), adopted by the organisations studied. According to ITGT (2007), the COBIT framework explicitly shows the difference between application controls and ICT general controls in order to simplify their difference to the organisation. As a result of their adoption by the Thai organisations, general controls were embedded in their ICT processes and services including systems development, change management, security and computer operations (ITGI 2007). Application control was embedded in business process applications to ensure completeness, accuracy, validity, authorisations and segregation of duties. Moreover, ICT control processes within the COBIT framework are defined by a complete set of high level requirements at the executive level and these too were clearly adopted in the Thai organisations studied. According to the respondents, the corporate plans needed to be effective so as to assist senior management directly influence the planning of ICT risk management.

Classification of ICT resources is also relevant to the current study which seeks to establish the existence and appropriateness of the ministry’s business continuity plans in the event of an unforeseen disaster occurring within the PFMS environment. It will also be worthy to establish the strength of the standards used in the classifying of the ministry’s ICT resources.

2.5.4. Operational ICT risk management plans and procedures

The respondents in the Thai organisations studied argued that operational managers also planned for successful ICT risk management. They further elaborated that an operational plan was used to define the procedures and methodology to deal with ICT risk at all of the operational levels. The respondents noted that an operational plan outlined the details of ICT risk management for each of the departments and that an operational plan was produced based on the corporate plan to expand the details of the realisation of a corporate plan throughout the organisation. The respondents revealed that the effectiveness of an operational plan derived from a number of
actions including defining and implementing information security control and audit processes, defining a clear outline of technical security measures and managing ICT project risks in each department. These determinations, the interview data showed, positively affected the success of ICT risk management planning in the corporate plan.

In the Kumsuprom et al (2008) case study, operational plans were the tools used as action plans in defining and implementing information security and audit processes in order to address issues pertaining to successful ICT risk management. It was also noted that there was need to align the corporate plan to the organisational policy in order to be able to outline the procedures to be exercised in the operational environment following the guidelines as set out in the COBIT Framework and the ISO/IEC 17799 Standard. Defining clear details of technical security measures in an operational plan was the other element that the respondents in the Thai case studies revealed in relation to establishing a plan for dealing with ICT risks at the operational level. The details of technical security required clarity to determine appropriate technical controls in each department. The outline of technical security measures emerged in each organisation from the ISO/IEC17799 standard, which stated that the details of control objectives in particular functions needed to be followed and adapted in the organisations (ISO/IEC 2005).

Managing ICT projects was also highlighted as an important element of an operational plan, in so far as software development treated ICT risk management on a project-by-project basis. Therefore, managing ICT project risk was considered in this study in terms of raising organisational awareness in ICT infrastructure changes or ICT project changes. The importance of managing ICT projects well was noted by Martin (2003), who stated that “ICT risk management is not only a prerequisite for successful project configuration, but it is a marketable competency”. Martin (2003) further argued that the methodology of ICT project risk management was not only used to manage an ICT project itself but also to manage operational and strategic risk embedded within the ICT projects.

It seems clear that the operational level plans are in fact action plans deriving from both the corporate and management level plans. The current study would also therefore seek to establish
whether the risk statements expressed in both the National ICT Policy and the management plan have been appropriately interpreted into action plans to effectively deal with successful ICT risk management.

2.6. Chapter Summary

The chapter reviewed the relevant literature in the field of ICT risk management in the context of the current research on ICT risk management in Zimbabwe with specific reference to central government’s Public Financial Management System. The chapter explains both the theoretical and empirical literature as well as the research gaps surrounding ICT risk management within organisations. In the next chapter, the research methodology used to carry out the study is explained. It highlights the research design, the instruments used in the research and methods used for data analysis.
CHAPTER III
RESEARCH METHODOLOGY

3.0. Introduction

This chapter provides perspective on the research design used to investigate the research problem with specific reference to research paradigm, research design, research strategy, research population and sampling design, data collection methods and techniques, and data analysis and presentation techniques. The methodology applied was meant to ensure that relevant data was collected in order to enable the researcher to address the research questions.

3.1 Research Paradigm

A research paradigm is an underlying philosophical approach taken to research. According to Neuman (2006:81-82), modern positivism adopts an essentialist orientation to reality and states that “Reality is real. It exists out there and is waiting to be discovered”. The implication is that the positivist approach allows the researcher to verify the theoretical interest (i.e. opinions, ideas and conceptual model) to be validated as a true model or concept (Lee 1991).

The interpretive approach, also known as the phenomenological approach, based on the early works by Weber (1864 -1920) believes that reality is socially constructed and fluid. The Robert Wood Johnson Foundation (2008) notes that the known is always negotiated within cultures, social settings, and relationship with other people. From this perspective, validity or truth cannot be grounded in an objective reality. What is taken to be valid or true is negotiated and there can be multiple, valid claims to knowledge.

Lee (1991:347) in contrast, argues that passing an empirical test can never verify conclusively that the theory of interest is true. This assertion is supported by the view that a positive decision can only temporarily support the theory, because subsequent negative decisions may always
overthrow it, a view alluded to by Popper (1968: 33) and Lee (1991: 347). In this regard, one imperative approach, the interpretive approach has been proposed to resolve the problem outlined above (Lee (1991) and Neuman (2006).

The Phenomenological approach is based on the way people experience the social phenomena in the world in which they live and is characterised by the following:

- It focuses on meanings that research subjects attach to social phenomena; (an attempt by the researcher to understand what is happening and why it is happening).
- It is concerned with the context in which events are taking place.
- The study of small samples may be more appropriate than large numbers as with positivism approach.
- Works mostly with qualitative data and uses a variety of methods to collect these data in order to establish different views of phenomena.

3.2. Selected Research Philosophy

This research adopted the phenomenological paradigm. This was done recognising the following parameters identified by Hussey and Hussey (1997) for this phenomenological paradigm:

- It tends to produce qualitative data: (this fitted well with the current study approach which sought to establish meanings that research subjects attached to ICT risk management within the PFMS environment through their experiences using the system as well as what they have learnt through observation).
- Data is rich and subjective: (the qualitative data was rich by nature, and the gathering process was subjective due to the level of involvement of the researcher).
• The location is natural: (the settings for this research were normal working environments rather than laboratory setting).

3.3. Research Design

Saunders et al. (2009), suggest that there are many types of research designs that are classified broadly into qualitative and quantitative researches. He further notes that quantitative research is basically about discovering patterns in data through providing answers to questions like who, what, where and how of the topic under study. Cooper and Schindler (2009) further explain that quantitative research attempts precise measurement of something. On the other hand, qualitative research includes an array of interpretive techniques which seek to describe, decode, translate, and otherwise come to terms with the meaning, not the frequency, of certain more or less naturally occurring phenomena in the social world (Cooper & Schindler, 2009). According to Creswell (2002) quantitative research differs from qualitative research in the sense that quantitative describes trends whereas qualitative focuses mainly on the provision of explanations. However, quantitative and qualitative research methods are often seen as opposing and polarized views. They are frequently used in conjunction with one another (Crossan, Lane and White, 1999).

This research adopted an exploratory research design because it provided the researcher with better ideas and insights into broader and vague problems concerning ICT risk management within central government’s PFMS environment. In addition exploratory design was appropriate to the current research as it aims at identifying the important and critical determinants of successful ICT risk management within the PFMS environment. The research was therefore focused on ICT risk management in relation to the adequacy of the policies and procedures currently in use as well as the adequacy of the infrastructure, in terms of how this affected successful ICT risk management. Literature search revealed that there is no previous research done on ICT risk management within central government’s PFMS environment from a technical perspective and hence exploratory design was appropriate.
3.4. Data Collection

There are many data collection instruments to consider. The researcher opted to use the depth interview guide and the self administered questionnaire to collect data from the respondents. Secondary data was collected through document analysis/review.

3.4.1. Depth interviews

Based on the literature review on ICT risk management within organisations, an in-depth interview guide was developed in order to adhere to the qualitative requirements of this study. Depth interviews were therefore held with senior management responsible for policy formulation and implementation as well as with line managers responsible for the business procedures platform and the network and hardware management. The interview was the most appropriate way of gathering data from senior management who on most occasions are time constrained as they have to attend scheduled meetings and rarely have enough time to respond to questions in writing. The interviews also gave the researcher an opportunity to ask follow-up questions as responses were being orally given. The highly structured question format was used primarily to gather socio-demographic information. For the most part, however, more open ended and less structured questions were used. The researcher asked the same questions to all the respondents, but the order of the questions, the exact wording, and the type of follow-up questions varied considerably.

Robson (1997) refers to an interview as a situation where one person talks and the other listens. The depth interviews served the purpose of establishing information relevant to the research and focused on the content specified by the interviewer. The interviews also allowed the researcher to observe non-verbal communication and make inferences. They also increased the response rate because the interviewer was in control of the information gathering process (Wegner, 1999). Interviews are time consuming and thorough but do produce more useful information for the research. Interviews may also raise concerns about bias, if not handled properly. They therefore, demand experience on the part of both the interviewer and interviewee.
According to De Vos et al. (2002: 302) the interview guide provides the researcher with a set of predetermined questions that guide the researcher’s thinking about the content of the interview that needs to be covered. Rubin and Babbie (2001) indicate that structured strategies to questions are aimed at ensuring that respondents answer the same questions in the same sequence. This also further ensures that the efficiency with which responses can be compared is maximised. The guided interview questionnaire had a total of ten (10) open ended questions. Since the research was qualitative, such questions allowed the interviewees to express their views independently

### 3.4.2. Questionnaire

A self administered questionnaire was also developed and utilised in gathering information from the respective Head Offices of the ministries and departments. The use of questionnaires in this study was cost effective and convenient in collecting data. Use of the questionnaire enabled the research to gather information from the respondents at about the same time. Self administered questionnaires can be handed out randomly wherever the target population can best be reached (Wegner, 1999). For this research, the questionnaires were personally hand delivered and collected to and from the respondents by the researcher. The questionnaire was meant to be completed by the respondents without assistance from the researcher. In this manner, the contribution of the researcher was kept to an absolute minimum, thereby avoiding the introduction of bias during the questionnaire completion process (De Vos et al. 2002: 302). The questionnaire also sought to establish the same views as did the depth interviews. Both instruments had the capability to produce consistent results at different times and with different user groups of the same system. The questions both in the questionnaire and in the depth interview guide were quiet straightforward and seemed relatively easy to answer for the respondents who, by virtue of their favoured positions, were expected to be well versed with the ICT risk management initiatives currently pertaining to the PFMS, thereby enabling easy scoring upon.
3.4.2.1 Questionnaire design

In the context of the research problem, objectives, approach and strategy, primary data was gathered through the use of depth interview notes as well as hand delivery and collection of questionnaires from the respondents. The questionnaire was designed and structured in a manner that ensured that all the five broad dimensions to the structured approach were taken care of. These broad categories were standards and frameworks implementation, policies and procedures formulation and implementation, strategic direction setting, human resources management and planning, security planning and technology.

3.4.2.2 Structure of the questionnaire

The questionnaire was structured in such a way that the first section of the questionnaire asked about the general demographic information of the respondent. Kangasharju (2000) argues that this section is important as statistical significance variance can be checked for all demographic variables that impact business performance and in this case, ICT risk management within central government’s PFMS environment.

3.4.2.3 Pre-testing of the questionnaire

The questionnaire was pre-tested on a sample of 6 individuals.(2 systems auditors, 2 systems analysts and 2 accountants). Gilbert and Churchill (1988) argue that a pre-test that is done through an interview enables the researcher to watch and see if people actually remember data requested of them. It also allows the researcher to see if some questions seem confusing or produce resistance and hesitancy among respondents. The pre-test therefore assisted in the identification of unclear and rather ambiguously formulated questions as well as testing the reliability of the selected instrument.
3.5. Document analysis/review

Records observation through inspection of system failure reports which are generated by the System to try and ascertain whether there was evidence of system failure being a result of system security breaches was not possible. The research established that a number of system breaches have been recorded but these could not be shared with the researcher without exposing attractive system weaknesses.

The Public Financial Management Act (Chapter22:19) and the current National ICT Policy as well as the Draft National ICT Governance Policy were however, reviewed. Emory (1980) stated that observation involves noticing what is going on around the research through systematic observation, recording, description, analysis and interpretation of people’s behaviour. It also extends to listening and reading. Observation can be classified into behavioural and non-behavioural observation (Emory, 1980:314). Behavioural observation looks at non-verbal analysis, linguistic analysis, extra-linguistic analysis and spatial analysis. Non-behavioural observation encompasses observation of non-human phenomena, like records, processes or activities. Both methods of observation however are useful as ways of gathering data.

Gill and Johnson (1997) classified observation into participant and structured observation. Participant observation involves the researcher participating fully in the lives and activities of the subjects and thus becomes a member of their grouping. The advantage is that it gives the researcher a better view of the social setting of the subject under study. The disadvantage is that it can pose difficult ethical dilemmas for the researcher. In structured observation the researcher is detached from the participants who are the subject of the study. The advantage is that the researcher can carry out simultaneous observations in different locations. The disadvantage is that the data is slow and expensive to collect. According to Leedy and Omrod (2001:195), the researcher should be as objective as possible, despite the method of observation used.
3.6. Target population

The study population is “that aggregation of elements from which the sample is actually selected,” (Rubin and Babbie 2001: 225). The selected population for this study was made up of people who had an ICT technical orientation and were in senior management and operational management positions within their ministries, departments or private companies who partnered the government in the PFMS project. The target population was therefore one hundred and twenty (120) senior management and senior operational staff from the Department of the Accountant General (PFMS Project Office) in the Ministry of Finance, Ministry of Finance System Audit Unit, key management and technical personnel from Dexel, Africom and Twenty Third Century Systems. The other members of the population were also drawn from the Systems Audit department of the Office of the Comptroller and Auditor General and from senior management and senior technical operational staff from the Ministry of Information Communication Technology, Postal and Courier Services.

3.7. Sample size

It would not have been feasible and realistic to consider each and every individual who is likely to bring risk to the central government’s PFMS environment. As such, it became necessary to examine only a sample of the population. A sample is a subset of the population that has been chosen for study. De Vos et al. (2002: 198) state that the individual units of analysis that are chosen should therefore represent the total study population that generates the research problem and toward which the final results will be generalised. A total of thirty (30) interview questionnaires, including those from face to face interviews, were administered to key informants from the above stated population. Fraenkel and Wallen (1996) suggest that a sample size of at least 10% of the target population is large enough to produce results that are representative of the population. The sample size percentage of the study was 25% of the target population.
3.8. Sampling procedure used in this study

According to Hill (1977), the two main categories of sampling are probability and non-probability sampling. Hill notes that these two main categories are often termed random and non-random sampling. The researcher therefore opted to use purposive sampling, a non-probability sampling method which can be considered as a combination of both convenience and or judgmental sampling techniques to select the subjects of the research. The researcher used this sampling method because it was convenient, low cost and because of the fact that respondents were expected to have some technical orientation in the ICT environment. These are the significant others in as far as ICT risk management within the central government’s PFMS environment is concerned. As such, other professionals such as accounting and human resources personnel, who do not have anything to do with ICT risk management within the PFMS environment were exclude from the grouping that formed the study sample.

The advantages of a sample are that it only involves a smaller number of the subjects and is more time efficient, less costly and is potentially capable of producing more accurate results because the researcher is able to maintain control over the smaller number of subjects. However, samples are prone to bias in the selection of subjects. This may lead to errors in interpretation of the results, thereby decreasing the applicability of the results beyond the subjects actually studied.

3.9. Research Data Validity and Reliability

Validity of a research is concerned with whether the findings are really about what they appear to be about. It is defined as the extent to which the data collection method or methods accurately measure what they were intended to measure (Saunders et. al. 2003). The questionnaire was pre-tested on a sample of 6 individuals. (2 systems auditors, 2 systems analysts and 2 accountants). Gilbert and Churchill (1988) argue that a pre-test enables the researcher to watch and see if people actually remember data requested of them. It also allows the researcher to see if some questions seem confusing or produce resistance and hesitancy among respondents. The pre-test therefore assisted in the identification of unclear and rather ambiguously formulated questions as
well as testing the reliability of the selected instrument. According to Saunders et. al. (2003), reliability refers to the degree to which a data collection method or methods will yield consistent findings, thus similar observations or conclusions would be reached by others undertaking the same research under the same conditions.

3.10. Data processing, analysis and presentation

Returned questionnaires from respondents, together with recorded depth interview notes constituted the primary data for the current study. The processing and analysis of these data entailed grouping the questionnaires’ questions into sub topics and have them analysed and discussed individually as per received responses. The research sought to only gather respondent comments and opinions regarding user understanding and practical experiences using the PFMS in an effort to respond to the research questions. The demographic data collected were analysed statistically using Microsoft Ms-Excel and the results were presented as explanatory statements.

3.11. Ethical Considerations

An accompanying letter of introduction regarding the purpose of the study, as well as an assurance of confidentiality, was drafted and included in every questionnaire. The purpose of the covering letter was to provide the prospective respondents with an orientation towards the purpose of the questionnaire, to enable subjects to fully comprehend the investigation and consequently be able to make voluntary and thoroughly reasoned decisions about their possible participation in the study. The research observed the principles of informed consent, respect for privacy, truthfulness, and avoidance of conflict of interest. Informed consent meant that the respondents were aware of the purpose of the research, how the data were to be gathered, and that they could exercise their rights to withdraw from the project at any time without penalty. In addition, this also meant that the respondents were aware of how the data would be published and that confidentiality would be maintained.
3.12. Chapter Summary

The survey approach was the main method used in the study. Selection of the sample was done using purposive sampling. However, this was done in such a way that would reduce bias whenever it was possible and mainly by using different approaches and different stages. Data was collected from in-depth interviews carried out, questionnaires distributed and secondary data sources. The next chapter, Chapter Four, presents the data obtained from the study, analyses the data and then interprets the data.
CHAPTER IV
DATA PRESENTATION AND ANALYSIS

4.0. Introduction

This chapter presents the results from the qualitative study, which determined ICT risk management in Zimbabwe with specific reference to central government’s Public Finance Management Systems (PFMS) environment. The main purposes of the study were to analyse the National ICT Policy that governs the use of ICTs in Zimbabwe, to ascertain the current profiles of ICT risk management within the central government’s PFMS environment and to establish the gaps within the central government’s ICT risk management initiatives for the PFMS. The study further sought to ascertain whether ICT risk assessment and mitigation initiatives currently in place were comprehensive and at the same time being fully operationalised within the central government’s PFMS environment. As such, the chapter will either confirm or deny the proposition that while a well-structured and adopted ICT risk management framework is of strategic importance to successfully deal with ICT risk management on the PFMS, operationalising such initiatives is critical. Explanatory statements were used to shade more light on the findings.

4.1. Survey response rate

The questionnaire was distributed to a total of 30 respondents as mentioned in the methodology section. The researcher had an 83.3% response rate. Therefore 16.7% did not respond hence they chose not to participate irrespective of the purpose of the study having been explained to them. However, the average response rate of 83.3% from both face to face interviews and questionnaires was high enough to enable meaningful conclusions to be drawn for the purposes of this research.
4.2. Respondent statistics by position level and department worked in

Analysis of the respondent data by position level revealed that there were more people at the operational level (52%) than at the managerial level (48%). Further analysis of the respondents by department they worked in indicate that those who worked in the Information Communication Technology Department were more than any other department (80%) among those who participated in this study. Those working in the Information Communication Technology Security and Risk Management Departments did not participate in this study. This could be an indication that there could be lack of segregation of duties irrespective of the fact that the duties are being carried out within the PFMS environment. For example, systems audit personnel felt they belonged to the ICT department whereas they could have classified themselves either as being from ICT Security or Risk Management departments.

4.3. Success factors in ICT risk management within the PFMS Environment

The review of the National ICT Policy established that the policy did contain the generic aspects that must be in an ICT policy for it to be effective in terms of addressing issues pertaining to successful ICT risk management within the PFMS environment. These were the development of organisational structure, organisational processes, organisational control and organisational ICT strategies.

4.3.1. National ICT Governance Policy

The research established that the current policy defines both the technological and the security directions in terms of the adoption of the use of ICTs in government business. In addition, the respondents also indicated the presence of a Business continuity plan which the ministry will use to face future and uncertain events regarding the loss of central government’s information assets.
A review of the current National ICT policy revealed that the policy document was drafted in 2005 and is therefore almost a decade years old. It is worth noting that the ICT sector involves fast changing technologies and is capital intensive. The current policy focuses on e-Readiness and e-Awareness and therefore fails to capture the tremendous telecommunications sector developments and the impediments to ICT sector further growth. For example the current policy does not address issues pertaining to inadequate communications infrastructure, ICT facilities, skills and data management systems. These are pertinent issues that need to be addressed if Zimbabwe is to remain in the bandwagon of the information age.

Such are some of the challenges in the telecommunications industry that call for periodic reviews of the policy that governs the use of ICTs in Zimbabwe. However, the responsible ministry now has a Draft Reviewed National ICT Governance Policy that awaits Cabinet approval. The Draft Policy places emphasis on, infrastructure development and management; research, innovation and industry development; policy streamlining, regulatory frameworks and institutional mechanisms; as well as capacity building and content development.

The research established that the purpose of the draft reviewed policy is to provide strategic direction and guidance for sustainable national ICT development through the development and application of ICTs in Zimbabwe. The draft policy fully indicates government’s serious intention to address issues pertaining to successful ICT risk management at both the national and ministerial levels through the statement “develop a legal framework that address issues related to cyber security, protection of data, intellectual property rights, e-transactions and ethical and moral rights”. However, most of the respondents instead chronicled activities such as access rights, use of root passwords and password system management. They therefore addressed the “how” part of the policy.

4.3.2. Organisational structure

The respondents noted that the current organisational structure (appendix “E”) is not ideal for appropriate allocation of responsibilities to employees with regard to ICT risk management.
They further noted that the major challenges with the current organisational structure are that the number of posts at the Deputy Director level results in work and responsibility overload to the few individuals. The respondents also observed that currently there is no Information Security Internal Audit Unit to assist with the reviewing of the information security program’s plans, policies, procedures and new key ICT risk management initiatives. The respondents further observed that currently, role allocation seems to be initiated from the top to be delivered down instead of being initiated from both ends so as to achieve consensus and come up with an ICT risk management plan for the whole organisation. They further observed that a consensus plan would provide details of ICT risk components which must be assigned to roles of relevant staff in the organisation. The sentiments of the respondents seem to be justified since a consensus plan would clearly spell out the responsibilities of staff dealing with ICT risk; the roles and tasks involved in controlling the ICT risks; ICT risk management procedures; and controlling the main components of ICT which the risks might threaten”.

Management seems to have long realised the shortcomings of the current organisational structure and have since drafted another organisational structure (appendix “F”), which seems ideal for properly addressing issues pertaining to successful ICT risk management with respect to the PFMS environment. The proposed organisational structure has been awaiting the Civil Service Commission’s (employing board) approval for the past three years. Such a long delay in correcting things seems to be confirming the problem statement that very promising government blueprints are in place but take too long to be operationalised or never get to be put into operation.

More positions at the Deputy Director level would create adequate leadership in the committee that will determine those responsible for directly controlling particular areas of ICT risk management. The tasks for dealing with ICT risks are classified into three critical areas of business direction, technological direction and security direction. Each of the three ICT risk management areas will be supported by a management committee. The respondents further observed that this would in turn assist the ministry to properly define responsibilities for specific matters in these three particular areas as well as also help the ministry to properly define its core
business and ICT processes. In addition, the respondents noted that the creation of an Information Security Internal Audit Unit would serve to ensure that information security efforts have a positive effect on the ministry’s performance in terms of ICT risk management as well as protecting the Ministry of Information Communication Technology, Postal and Courier Services from harm through the reviewing of the information security program’s plans, policies, procedures and new key ICT risk management initiatives. The Information Security Internal Audit Unit will also be responsible for safeguarding stakeholder interests in as far as they get affected by the implementation of ICT risk management within the PFMS environment.

A review of the proposed organisational structure in the light of the respondent sentiments seems to suggest that ICT risk management treatment would be a focus at both the management and the operational levels and that each level will be responsible for different tasks related to defining the business direction, the technological direction and the information security direction. The management level ICT risk statement will affect the Ministry of Information Communication Technology, Postal and Courier Services as a whole while the operational level will come up with plans that address the technical aspects of the management plan. Thus both the top-down approach and the bottom-up approach will be implemented as part of a consensus agreement on how to deal with ICT risk management. Simply put, the respondents’ statements seem to be in line with the COBIT Framework guidelines.

4.3.3. Organisational processes

It was established that the OS was configured to comply with COBIT to aid management directives to the operational level. It was also established that the operational level had the SAP Business Objectives Governance, Risk and Compliance Standards at its disposal. However, there was no evidence of the management risk statement having been effectively communicated to the operational level since there was very little work undertaken toward attaining successful ICT risk management within the PFMS environment. The Ministry of Information Communication Technology, Postal and Courier Services seems to be mostly focused on IT issues rather than on risks related to the business. It also became apparent that despite both the current and the
reviewed draft National ICT policies having a specific ICT development and management tentacle to which ICT risk management could be tied to, the strategic plan initiatives to deal with ICT risk management have never been effectively executed. For example, the first annual risk assessment was due in 2010 but no single risk assessment exercise had been undertaken over the period under review. The same applied when it came to the issue of drawing up audit plans, as well as implementing and reviewing them annually.

4.3.4. Organisational ICT strategies

4.3.4.1. Strategic Plan

The respondents indicated that management has the responsibility to draw up the relevant policies to deal with successful ICT risk management within the PFMS environment. Further, and to strengthen this understanding, the respondents also observed that ICT risk management policies are not generated by the operational level. However, a review of the System Audit Management Letters over the years 2010 through to 2014, indicated that the Strategic Plan in place did not adequately address issues pertaining to investment or operational budgets, funding sources, sourcing strategies and acquisition strategies. The same management letter also noted that the absence of an IT Strategic Plan could lead to non-alignment of business objectives and IT, further noting that if the plan is not developed, management might not set aside adequate resources for implementation of such a plan and this may result in non achievement of strategic goals and objectives.

The research established that there is a Road Map with which to take the PFMS forward. However, whilst there is a PFMS Road Map which constitutes the strategic plan for the management and maintenance of the PFMS, there was no evidence to support that the same was being continuously updated to take into account new developments in the operating environment as well as addressing new issues pertaining to successful ICT risk management within the PFMS environment. The research also revealed that the Road Map was developed by external consultants with the blessings of senior management. There was also no evidence to support the
fact that this “Road Map” had been made known to all staff in the various departments of the
Ministry of Information Communication Technology, Postal and Courier Services. Information
of such a strategic nature needs to effectively communicated to staff.

4.3.4.2. Risk Assessments

According to the Ministry of Information Communication Technology, Postal and Courier
Services’ Strategic Plan for the period 2010 to 2014, the first risk assessment report was due in
March 2010 but no risk assessments had been undertaken on the PFMS over the period under
review. Senior management revealed that no Risk Assessment Framework had as yet been
developed due to capacity constraints, resulting in the risk assessments not having been
performed for the PFMS. The research also established that resources supporting critical
operations to maintain business processes had not been identified, classified and documented.
Information resource classification is a process in which ICT resources are identified and
classified according to criticality to ensure that the most critical resources are adequately
insured/protected. These resources included computer hardware, software, supplies, system
documentation, office facilities and networks. However, it was established that most critical
resources were covered under Service Level Agreements with service providers. It was also
noted that despite there being signed Service Level Agreements with the service providing
companies, there were no corresponding Service Level Guarantees to the same effect.

4.3.4.3. Business continuity plan

The respondents observed that it was critical for the Ministry of Information Communication
Technology, Postal and Courier Services to have a business continuity plan in place to enable
resumption of business soon after a disaster. They indicated that one such plan existed within the
PFMS environment. The research established that the disaster recovery site was out of Harare.
However, the respondents observed that the current plan, though approved by management,
tested and communicated to staff, did not adequately address issues pertaining to clearly
assigning responsibilities for recovery, identification and classification of critical information
resources and identification of business processes that should be recovered first. The research established that the Ministry of Information Communication Technology, Postal and Courier Services was in the process of sourcing funds to enable it to hire a consultant to carry out this assignment.

4.3.4.4. Standards and Framework Implementation

Most of the respondents did not respond to this question. Only 32% of the respondents were aware that the Sun Solaris operating system drives the Oracle Database on which the Public Financial Management System sits. It is best practice that management levels possess this knowledge in order to be able to assess the risks to its information assets as it would to legal, regulatory, financial or operational risk. Defining and communicating the ministry’s attitude and approach to risk management is crucial. This will assist management in communicating its risk appetite statement and information risk management policy across the PFMS environment to ensure that employees, contractors and suppliers are aware of the organisation’s risk management boundaries.

Despite the respondents having an ICT technical orientation, similar sentiments were also revealed with respect to ISO/IEC standards having been implemented in order to mitigate, avoid, prevent or control risks. Only 44% mentioned standards or frameworks such as COBIT, SAP GRC 10.0 and ISO/IEC 17799 standards that were relevant when dealing with ICT risk management for the PFMS. The majority (56%) did not respond on this aspect of the study.

The research established that the OS was configured to comply with COBIT as well as SAP Business Objects Governance, Risk and Compliance (GRC 10.0) Standards, in order to deal with ICT risk management and planning within the central government’s PFMS environment. In contrast, some respondents showed that they did not have knowledge of standards or frameworks that management implemented in order to deal with ICT risk management and planning with respect to the PFMS. This lack of knowledge on standards among operational staff was however explained through depth interviews which indicated that there were no challenges with
configurations as these configurations are outsourced from specialist and reputable companies who have been delivering commendable services in order to protect their reputations and hence guarantee themselves future contracts. Therefore ICT risks likely to be emanating from improper configurations were unlikely to occur.

4.4. Identification of sources of ICT and IS risks within the PFMS environment

The research established that the area regarding access control was not being appropriately managed. The respondents observed that too many users had access to critical profiles such as data dictionary maintenance, modifying critical tables, maintaining of technical settings and production client setting maintenance. It also became apparent that the granting of such access rights was not in line with the users’ roles and responsibilities. These profiles enabled them to perform duties not in line with their defined roles and responsibilities thereby compromising segregation of duties. Further, the research established that this was so due to skills flight from the Ministry of Information Communication Technology, Postal and Courier Services.

4.4.1. Pirated software

The respondents advised that there was a proliferation of pirated software and other applications on individual work stations. This suggested that the ICT function was again not being properly managed. Ideally, the ICT function should have been appropriately controlled by managing performance and capacity; managing the configuration; managing problems; managing data; managing operations; monitoring and evaluating IT performance; monitoring and evaluating internal controls; ensuring compliance with external requirements; and providing ICT governance, as illustrated in the COBIT framework. The research established that the Ministry of Information Communication Technology, Postal and Courier Services had the necessary software and control mechanisms to prevent the loading of pirated software onto its work stations but these were not being consistently applied within the PFMS environment thereby exposing itself to risks. These research findings confirm previous research findings by McEvoy and Whitcombe (2002) and Kumsuprom et.al (2008), who conclude that ICT risks result from
uncontrolled practices including the use of pirated applications and software, improper or incomplete software licensing, poor protection of intellectual property and from incomplete software maintenance and updating.

4.4.2. Information security awareness

The research established the there were a number of indicators to measure the level of information security awareness and preparedness with respect to ICT risk management on the PFMS. These had to do with what policies management had put in place so as to protect central government’s information assets. Correctly configuring the operating system, the networking operating system, the hardware and the business software would be the first step. Respondents in the study indicated that management correctly configures the OS, the networking OS, the hardware and the business software and further noted that these configurations were outsourced from specialist and reputable companies. The respondents further indicated that there were no challenges with configurations as the companies hired delivered commendable services in order to protect their reputations and hence guarantee themselves future contracts.

On the other hand, the research established that there were a number of concerns with regard to information security awareness within the PFMS environment. For example, it was established that the root password was shared by too many people who also included staff from the partnering companies. In the event of information deletion, it may have become difficult to trace the individual responsible. In addition, the Information Security Policy in place showed that it had been crafted in 2007, but had not been approved by management and had not been formally communicated to staff in different departments. Previous research by Hughes (2006b); Hilton (2009) and Martinez et al. (2010), indicate that data protection and privacy in relation to employee behaviour related to the control of the level of personnel access rights of employees to information (e.g. specified information related to staff’s job descriptions), to information technology (e.g. specified software and applications related to staff’s job descriptions) and to systems (e.g. a specified module related to staff’s job descriptions).
The respondents also noted that the use of passwords to limit access into the system by unauthorised personnel seemed to be no longer an effective access control measure. They therefore advocated for use of biometric access controls such as fingerprint and face recognition as well as voice recognition.

4.4.3. Data input validation

The research further established that input data validation for correctness, appropriateness and corruption through deliberate acts was achieved through Access Risk Management resident on the system. The SAP Business Objects Access Control unifies access risk analysis and remediation, business role management, compliant identity management and emergency privilege management. It therefore provided comprehensive management oversight and performed effective and complete audits. The respondents indicated that validation checks had to pass through Development and Quality Assurance (QAS) prior to being transported to Production. There were therefore fewer chances that input data could easily be intercepted and manipulated.

The research also established that, of major concern to system security was the fact that both ICT and IS security controls, were sometimes switched off in order to create storage to carry out other assignments. A number of system breaches during such off-times had been recorded but these could not be shared with the researcher without exposing attractive system weaknesses. Records observation was therefore not possible. However, according to the respondents, exploitation of the weaknesses could only be exercised by insiders who were privy to that knowledge and had history of previous system breaches. All the same, the fact remained that accountability for breaches and the negative outcomes occurring when audit logs and trace files were switched off could not be associated with a particular individual. It is therefore critical to note that the ICT and IS security areas require management at both the management and operational levels to follow guidelines for its proper management based on the COBIT framework, and the GRC 10.0 Standards respectively.
4.4.4. Human resources

The research established that generally, the respondents agreed that human resources ICT risk management initiatives do prevail within the PFMS environment. For example, most of the respondents noted that management defines employee roles and observed that employee responsibilities regarding information governance policy with respect to ICT risk management on the PFMS were also well defined. Further, the respondents noted that management properly defines employee roles in its information governance policy and in its information security governance policy. However, the respondents noted that segregation of duties was in most cases compromised since staff were often asked to perform duties that were not aligned to their job descriptions. Senior management conceded to this weakness giving staff shortages as the main reason.

Despite the cited weakness, it was encouraging to note that almost all the respondents were aware of the existence of the Official Secrets Act. They further observed that management declared terms of employment with regard to information confidentiality and non-disclosure of that information to third parties. However, there was no evidence to support the fact that these controls with respect to increasing ICT risk awareness with respect to the PFMS among the employees were being effected. For example, signed acknowledgement forms by employees would have sufficed as evidence of the employees having read the Official Secrets Act. This goes further to amplify the fact that many instruments that could assist management to prevent, control, mitigate and avoid ICT risks were not being put to practical use thereby compromising system security.

4.4.5. ICT risk awareness

ICT risk awareness and ICT security risk awareness is normally achieved through proper induction of new recruits, training programmes on new developments and periodic refresher courses. Most respondents observed that such training programmes were essential in order to avoid, prevent and mitigate ICT risks that emanated from human behaviour in the workplace.
However, the research established that essential training was not being availed to staff fast enough so as to enable them to catch up with the dynamic technological environment. In order to make employees more appreciative of the system vulnerabilities within the PFMS environment, courses such as Basis, Oracle, Linux and Cisco administration as well as ABAP programming should be offered more often. However, the respondents indicated that such courses were not offered locally and were therefore expensive. Further, research findings showed that human resources must be trained and educated in order to gain a thorough understanding of the organisational vulnerabilities and of the resources needed to secure organisational information and systems. Inadequate funding was cited as the main drawback hence the Ministry of Information Communication Technology, Postal and Courier Services had not been able to avail such training programmes more often in order to increase staff’s information and security awareness.

4.4.6. System access rights management

System access rights management is an area in which many enterprises struggle to effectively manage risks. In this respect, segregation of duties and excessive access rights have been cited as the major contributors to fraud and qualifying audit findings. Respondents in the current study observed that change and removal of access rights upon change of employment and termination of employment, respectively, were being accordingly effected. However, it is worth noting that timing of these actions is most critical. Informing the responsible office of any such changes should be done fast enough or abuse of the system by employees will occur. For example, the office responsible for granting and withdrawal of system access rights noted that an employee who had resigned was still having access rights and supposedly conducting transactions long after having resigned. This suggests that a single individual may have the capacity to successfully execute fraudulent transactions thereby exposing government to the risk of financial loss.

The respondents also observed that there were many instances of computer abuse by staff. They noted the proliferation of pirated applications and software on individual staff workstations as
well as over usage of internet facilities. As a result, viruses were an everyday thing within the working environment. Further, the respondents observed that although remedial action was always taken to remove the viruses, no charges had as yet been levelled against offenders so as to discourage potential offenders from abusing the system. Given such a scenario, it would again seem to suggest that, despite there being adequate statutory instruments such as the disciplinary regulations; the same enabling instruments were not being brought into practical use within the PFMS working environment thereby compromising system performance. Literature suggests that applying the deterrence theory within the operating environment could assist in discouraging staff from abusing the system. Furthermore, continuous deployment of the Network monitoring software and the Sophos antivirus software would further discourage staff from abusing and further exposing the system to both ICT and IS risks.

4.4.7. ICT infrastructure and technology within the PFMS environment

The respondents indicated that the technology in place for the PFMS compared favourably with that of other similar institution both locally and in other Sub-Saharan countries. In relation to successful ICT risk management for the PFMS, the respondents observed that management provided sufficient networking connection to users as well as sufficient personnel access to the system. They further indicated that management properly managed several types of operating software in order to generate data and information in the same pattern. Additionally, the respondents indicated that management also provided all applications with legal of use.

On the other hand, the research established that the major concern in this area was the fact that most licensing payments were in arrears by between twelve (12) to eighteen (18) months. They were of the opinion that missed upgrades due to non-payment of license fees may open up the system to operational risks as well as missing on new system functionalities. The importance of the PFMS to central government cannot be over emphasised. Management should therefore continuously lobby with Treasury so as to ascertain that adequate budget support funds are timeously availed. The National ICT Governance Policy as well as the Ministry of Information Communication Technology, Postal and Courier Services’ Strategic Plan clearly indicates that
government respects the issue of intellectual property rights and therefore payment of licensing fees would be one way to show compliance to such an understanding.

The study also established that capital budget allocations for the PFMS over the period under review have not been encouraging. Management indicated that this has been the major cause of not having attained successful ICT risk management within the PFMS environment. It was further established that the unavailability of adequate funding was responsible for there being need to sometimes switch off some controls within the system in order to create space for other system assignments. It was also established that although the African Development Bank (AfDB) was giving assistance in this respect, its releases were not timeous. For ample, the AfDB had promised to procure servers for the PFMS in February 2014 but up to the present moment, nothing has materialised. It also became apparent that the World Bank (WB) is also interested in supporting the PFMS. However, it was noted that the WB has just recently started doing its system status of the PFMS assessments and had indicated that its report would be due end February 2015. Furthermore, its turnaround time cannot again be guaranteed in terms of being timeous. Under such circumstances, the ministry should consider adopting a phased risk based approach toward attaining successful ICT risk management within the PFMS environment based on Treasury expenditure targets and only accelerate implementing risk management initiatives when assistance is practically guaranteed.

4.5. Tools that can be identified in compiling the ICT risk management framework for the PFMS

4.5.1. Strategic level plans

The presence of IT control and audit plans, providing an overview of IT applications and IT security as well as providing an overview of ICT risk management methodology in a management plan are indications that management has the intention of addressing issues pertaining to successfully dealing with ICT risk management within the PFMS environment. The respondents indicated that such plans existed within the PFMS environment.
It was also established that the Ministry of Information Communication Technology, Postal and Courier Services’ management plan is in the form of a five (5) year strategic plan for the period 2010 to 2014. In this strategic plan, the intentions to address issues pertaining to ICT risk management are indicated through plans to conduct annual risk assessments, undertaking of three systems audits annually and annual evaluation of internal controls and procedures. The Information Systems Internal Audit Unit was assigned to spearhead the crafting of the necessary documentation. However, because the new organisational structure had not been approved by the employing body, the IS Internal Audit Unit does not exist. This further amplifies the problem statement that very promising government blueprints are in place but take too long to be operationalised or never get to be put into operation. This seems to suggest that generally, implementation of positive ICT risk management initiatives within the PFMS environment, but with financial connotations, over the period under review have not been entertained.

4.5.2. Operational level plans

The operational level plans are in fact action plans to address the technical aspects of the management level plans. The research established that the management level plan has a well-defined Risk Statement that should serve as the operational level ICT risk management methodology in the operational level action plans. However, reference to the section on risk assessments show that these assessments have never been undertaken on the PFMS. The absence of a risk assessment framework and audit plans at the operational management level therefore seem to suggest that ICT risk management for the PFMS is an issue that management has in mind but has not seriously considered implementing. Under such circumstances, it would seem that there has been as yet, no significant incident to indicate to management that there is need to seriously consider implementing appropriate ICT risk management initiatives.

While the respondents observed that the management has established information security control and audit in the action plan for the specific departments through its risk statement, the study established that only a few policies (action plans) have so far been developed toward
attaining successful ICT risk management within the PFMS environment. These policies include the internet policy, the information security and the general security policies as well as the network and hardware policies. These policies would go a long way in assisting management successfully deal with ICT risk management within the PFMS operating environment. However, the operational management advised that these policies had not as yet been put into operation and neither had they been communicated to the central government’s PFMS users. Given such an understanding, one would be forgiven if they once more echoed the problem statement.

Furthermore, the research established that network monitoring software to monitor user activities within the PFMS environment had been installed. This software enables the operations management to see, who among all the users had visited what cites and what activities they undertook on their workstations. This security initiative, according to the operations management, has not been made known to the users. However, other than blocking the users from visiting their desired cites, no action for system abuse was undertaken. In addition, it was also established that the Sophos antivirus software was used to control the loading of private applications onto employee workstations. Again as with the use of the network monitoring software, the use of Sophos was also not communicated to the users.

The failure to communicate these initiatives to the users also raises ethical issues. Management should therefore consider compiling a comprehensive code of ethics to be applied within the PFMS working environment. A code of ethics outlines a set of fundamental principles. These principles can be used both as the basis for operational requirements (things one must do) and operational prohibitions (things one must not do). Typically, a code of ethics is founded on a set of core principles or values and is not designed for expedience. These principles are illustrated with behavioural examples. Those subject to the code are expected to understand, internalise, and apply the examples in situations the code does not specifically address. Organisations expect that the principles, once communicated and illustrated, will apply in every case, and that failure to apply the principles can be a cause for disciplinary action.
4.6. Chapter Summary

The chapter presented the findings of the research on ICT risk management with respect to successful ICT risk management in the central government’s PFMS environment. The survey undertaken assessed the qualitative aspects of ICT risk management with particular focus on the ICT risk management practices as deduced from the review of relevant literature in Chapter 2. Chapter 5 draws conclusions based on the findings presented in this Chapter (Chapter 4).
CHAPTER V

CONCLUSIONS AND RECOMMENDATIONS

5.0 Introduction

The chapter summarises the findings of the study, the methodology of the study and the recommendations thereof to the beneficiaries of the study on ICT risk management practices on central government’s Public Financial Management System environment for the period 2010 to 2014. The chapter will also proffer conclusions on the findings obtained from the study as well as areas for further research.

5.1 Summary of research findings

The research set out to evaluate the ICT risk management practices within Zimbabwe Central Government’s Public Financial Management System Environment for the period 2010 through to 2014. This was achieved through analysing the National ICT Policy that governs the use of ICTs in Zimbabwe, ascertaining the current profiles of ICT risk management within the central government’s PFMS environment and establishing ICT risk management gaps within the central government’s ICT Risk Management Framework for the PFMS. Furthermore, it was an implied objective of the study, to establish the existence of a Risk Assessment Framework and whether the Risk Assessments were being carried out on a regular basis and when systems and other conditions change.

From the data gathered through desk research, questionnaires and depth interviews, the research concluded that the ministry is mostly focused on ICT issues rather than on risks related to the business. Literature according to Coles and Moulton (2003) supports this finding that most organisations focus on ICT issue rather than risk management. It is evident that the National ICT Policy clearly addresses issues dealing with successful ICT risk management while the Management Plan (Strategic Plan) also has clear risk statements that should enable the
operational level to make clear risk management action plans. However, the current National ICT Policy is almost a decade years old.

The research has established that ICT risk management strategies do prevail but these are not consistently being applied within the central government’s PFMS environment. Further, it was established that there is no risk assessment framework, that ICT resources were not appropriately classified and that the current organisational structure is not conducive for the implementation of ICT risk management initiatives. In addition, the research established that both new and existing ICT risk management policies and procedures were not being effectively operationalised within the PFMS environment. It was further established that most of the ICT risk management initiatives were not communicated to all stakeholders. The findings further show that despite there being signed Service Level Agreements with the service providers, there were no corresponding Service Level Guarantees to the same effect.

The research also established that human resources management and planning in terms of successful ICT risk management within the PFMS environment was not at its best. For example, the general deterrence theory was not being put to use within the PFMS environment in order to reduce the ICT risks as alluded to by Straub and Welke (1996), who state that “active and visible policing is thought to lower computer abuse by convincing potential abusers that there is too high a certainty of getting caught and being punished severely”. Further, the findings show that human resources must be trained and educated in order to gain a thorough understanding of organisational vulnerabilities and of the resources required to secure organisational information and systems (Straub and Welke 1996). In addition, the research also indicates that segregation of duties was in most cases compromised since staff were often asked to perform duties that were not aligned to their job descriptions. The research further notes that the failure to communicate change initiatives to the stakeholders also raises ethical issues.

It was also established that there were no issues with regard to systems configurations as well as input, processes and output validation controls. However, serious issues arise in the granting of system access rights, periodic reviews of both the ICT and IS security policies as well as the
periodic switching off of the audit logs and trace files in order to create capacity to do other assignments.

The research also revealed that no system abuse deterrence countermeasures against offenders had been exercised within the PFMS environment. However the researcher could not establish the reasons for hesitation by the operational level management to be seemingly dragging its feet in terms of operationalising the ICT risk management initiatives that are resident within the system and those that they have developed. The research also established that there have been a number of system breaches but these could not be discussed with the researcher for fear of exposure.

5.2. Conclusions

The research set out to evaluate the ICT risk management practices within Zimbabwe Central Government’s Public Financial Management System Environment for the period 2010 through to 2014. This was achieved through analysing the National ICT Policy that governs the use of ICTs in Zimbabwe in terms of its appropriateness in addressing ICT risk management issues within the PFMS environment, ascertaining the current profiles of ICT risk management within the central government’s PFMS environment and establishing the ICT risk management gaps within the central government’s ICT Risk Management Framework for the PFMS. Based on these objectives, the following conclusions were drawn:

5.2.1. To analyse the government ICT Policy that governs the use of ICTs in Zimbabwe in terms of its appropriateness in addressing ICT risk management issues within the PFMS environment.

- The current policy focuses on e-Readiness and e-Awareness but fails to capture the pertinent issues such as the tremendous telecommunications sector developments and the impediments to ICT sector further growth while the draft reviewed policy that awaits Cabinet approval comprehensively provides strategic direction and guidance for
sustainable national ICT development through the development and application of ICTs in Zimbabwe.

5.2.2. To ascertain the current profiles of ICT risk management within the central government’s PFMS environment.

- Most of the ICT and IS risks within the PFMS environment emerge from poor access rights management, inconsistent application of ICT and IS security controls as well as the ministry’s inability to provide essential training to staff fast enough so as to enable them to catch up with the dynamic technological environment.

5.2.3. To determine ICT risk management gaps within the central government’s ICT Risk Management Framework for the PFMS.

- There is need to develop a comprehensive risk assessment framework to enable the conducting of risk assessments on a regular basis. ICT resources also need to be appropriately classified while Service Level Guarantees need to be signed with the vendor companies that the ministry signed Service Level Agreements with. It is critical that both new and existing ICT risk management policies and procedures are operationalised within the PFMS environment. More ICT risk management policies need to be developed in all areas of operations that currently do not have ICT risk management policies. All change initiatives need to be communicated to the stakeholders.

5.2.4. General conclusions

- Both the Draft Reviewed National ICT Policy and the current National ICT policy address issues pertaining to successful ICT risk management issues at both the National and ministerial levels.
• ICT and IS risks within the PFMS environment emerge from poor access rights management, inconsistent application of ICT and IS security controls as well as the ministry’s inability to provide essential training.

• There is no risk assessment framework and no risk assessments have been undertaken within the PFMS environment. The Business continuity plan is not comprehensive while there are no Service Level Guarantees with the vendor companies that the ministry signed Service Level Agreements with. Both new and existing ICT risk management policies and procedures are not being consistently operationalised within the PFMS environment. Change initiatives are not being fully communicated to the stakeholders.

5.3. Recommendations

5.3.1. ICT risk management strategy and policy issues

There is a need to provide a clear framework for assessing ICT risks. This will enable assessment of the ministry’s current capabilities in all key areas of ICT risk management. Key priorities for reaching world class levels in ICT risk management must be the focal point. The ministry’s ICT risk strategy must state how the risk policy can be tightened to reflect better, how the ministry intents to guard against unauthorised access by service providers and by rogue service provider employees. The proposed organisational structure will aid the Ministry of Information Communication Technology, Postal and Courier Services in its efforts to attain successful ICT risk management within the PFMS environment. The ministry should therefore continue to lobby with the employing body to have the proposed structure approved as well as with Treasury for availing funding for the filling of the currently vacant posts. In addition the ministry must also adopt a risk based approach in the procurement of ICT resources including services. Further, ICT risk management policies must be reviewed constantly so as to capture the complex growth in ICT risks due to increased adoption of ICTs and the fast changing technology. Political will in this respect is guaranteed hence the ministry must solicit new ways with which to fight the bureaucratic tendencies that have resulted in the delays in the approval of the proposed
organisational structure and the launching of the Reviewed National ICT Governance Policy. It is also critical that all change initiatives are communicated to stakeholders.

5.3.2. Human resources management and planning issues

Roles, responsibilities, authorities and membership of key ICT risk management committee as well as those of the operational staff assigned the ICT risk management responsibilities need to be clearly defined. Responsibility for any act or omission should therefore be fixed; hence control by procedure is fundamental. The deterrence theory should be put to use within the PFMS environment in order to reduce the ICT risks emanating from employee abuse of the system. Essential training courses such as Basis, Oracle, Linux and Cisco administration as well as ABAP programming should be offered more often. Training only a few staff on such courses should be considered. Further, those having received the training will again need to be given the Train the Trainer course so that on return they will be able to train the rest of the staff in-house.

5.3.3. Regulatory compliance and corporate governance (security) issues

The SAP Business Objectives Governance, Risk and Compliance (GRC 10.0) Standards must be fully operationalised within the PFMS environment. Use of ICT controls and Audit Plans must no longer remain management’s intention to successfully deal with ICT risk management on the PFMS, but must be practically exercised soonest. Adequate storage facilities for both data and information need to be procured in order to do away with the need to sometimes switch off Audit logs and trace files. Risk managers should be on the forefront in terms of risk identification, assessment and resolution after taking into account all the inherent risks within the PFMS environment.

5.3.4. Business continuity management

A comprehensive Business continuity management plan in which resources supporting critical operations to maintain business processes after a disaster needs to be put in place as a matter of
urgency. There is therefore need to appropriately identify, classify and document such resources. Information resource classification is a process in which ICT resources are identified and classified according to criticality to ensure that the most critical resources are adequately insured/protected.

5.4. Recommendations for further research

Further ICT risk management studies can be carried out on all other government and quasi-government systems to establish the various system weaknesses within these organisations by also assessing the adequacy of the ICT risk management initiatives in place using standards. There is need to pursue such investigations further so as to establish whether the increasing rate of cybercrime within these institutions can be attributed to weak ICT and IS risk management. A lot of areas under ICT and IS risk management and their impact on organisational systems performance have not been explored in the Zimbabwean context, hence there is need to investigate causes and effects. This will help assess the preparedness of these institutions in introducing new ICT risk management techniques as cloud computing is fast becoming the next in-thing.
References

Besanko, Dranove and Shanley, (1996) Failures in Risk Management. Federal Reserve Bank of Boston,


ISO/IEC 27001 Services for information security management: Indian Journal of Science and Technology Vol. 5 No. 2 (Feb 2012).


McEvoy and Whitcombe (2002); Structured Risk Analysis Infrastructure Security Lecture Notes in Computer Science Volume 2437, 2002, pp 88-103


Popper (1968), The Logic of Scientific Discovery, Hutchinson & Co.


APPENDICES

Appendix “B” Letter of invitation to participate in the study

Dear Sir/Madam,

Ref: Invitation to participate in a survey on ICT Risk Management on the Public Financial Management System (PFMS).

I write to invite you to participate in my research project on the investigation of structured approaches to ICT risk management with regard to the Government of Zimbabwe’s PFMS.

I am a Masters of Business Leadership student with the Bindura University of Science Education, undertaking the said research as part of my degree qualification requirement. The research findings may contribute to a better understanding of ICT risk management theory and practice that may lead to successful ICT risk management in Government.

You being an important stakeholder are being invited to participate in this research by answering the questions on this form. Your responses will be treated as grouped data and will be used for academic purposes only. Participation in the survey is completely voluntary, and has no perceivable risk or disadvantages as I seek, only your comments and opinions regarding your understanding and practical experiences using the PFMS.

Yours faithfully,

Tendai Knowledge Mudzimuirema
PART A (Respondent profile and job functions)

1. Which position level are you in?

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
<td>Management level</td>
</tr>
<tr>
<td>b</td>
<td>Operational level</td>
</tr>
</tbody>
</table>

2. Which department are you responsible for?

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
<td>Internal Audit department</td>
</tr>
<tr>
<td>b</td>
<td>Information Communication Technology department</td>
</tr>
<tr>
<td>c</td>
<td>Information Communication Technology Security department</td>
</tr>
<tr>
<td>d</td>
<td>Risk Management department</td>
</tr>
<tr>
<td>e</td>
<td>Accounting department</td>
</tr>
</tbody>
</table>

Section B : Standards and Frameworks Implementation

3. Which database system and operating system (OS) drive the PFMS?

4. To which standards is the OS configured to comply with ?.
Section C : Successful ICT risk management with respect to the PFMS

5. In what way does the ICT policy indicate government’s intention to address issues pertaining to successful ICT risk management on the PFMS?

6. Why should the operational level be involved in the formulation of an ICT risk management policy for the PFMS?

7. What is the purpose of a Business Continuity Plan with respect to ICT risk management on the PFMS?

8. What has management done to increase ICT and IS risk awareness within the PFMS environment?
9. What changes would you make to the current organizational structure to make it ideal for the implementing of successful ICT risk management initiatives for the PFMS?

............................................................................................................................
............................................................................................................................
............................................................................................................................
............................................................................................................................
............................................................................................................................
............................................................................................................................
............................................................................................................................
............................................................................................................................
............................................................................................................................
............................................................................................................................
............................................................................................................................
............................................................................................................................
............................................................................................................................
............................................................................................................................
............................................................................................................................
............................................................................................................................
............................................................................................................................
............................................................................................................................
............................................................................................................................
............................................................................................................................
............................................................................................................................
............................................................................................................................

10. What have been your experiences in terms of system abuse by staff as a result of the current access control rights initiatives?

............................................................................................................................
............................................................................................................................
............................................................................................................................
............................................................................................................................
............................................................................................................................
............................................................................................................................
............................................................................................................................
............................................................................................................................
............................................................................................................................
............................................................................................................................
............................................................................................................................
............................................................................................................................
............................................................................................................................
............................................................................................................................
............................................................................................................................
............................................................................................................................
............................................................................................................................
............................................................................................................................
............................................................................................................................
............................................................................................................................
............................................................................................................................
............................................................................................................................

11. Updating of risk registers, reviews of Information Security (IS) architecture and IS awareness training will assist management to have a firm control on ICT risks. How consistent is the application of these security policies within the PFMS environment?

............................................................................................................................
............................................................................................................................
............................................................................................................................
............................................................................................................................
............................................................................................................................
............................................................................................................................
............................................................................................................................
............................................................................................................................
............................................................................................................................
............................................................................................................................
............................................................................................................................
............................................................................................................................
............................................................................................................................
............................................................................................................................
............................................................................................................................
............................................................................................................................
............................................................................................................................
............................................................................................................................
............................................................................................................................
............................................................................................................................
............................................................................................................................

12. Why are the systems hardware, networking and software configurations being outsourced for the PFMS? 

............................................................................................................................
............................................................................................................................
............................................................................................................................
............................................................................................................................
............................................................................................................................
............................................................................................................................
............................................................................................................................
............................................................................................................................
............................................................................................................................
............................................................................................................................
............................................................................................................................
............................................................................................................................
............................................................................................................................
............................................................................................................................
............................................................................................................................
............................................................................................................................
13. The Business Procedures Platform Manager says that “the use of passwords to limit access into the system by unauthorised personnel seems to be no longer an effective control measure”.

What should management do to address such concern?

14. How do you ensure that input, processes and output validations do not malfunction in the production platform?

15. How does the organisational technology compare with that of similar institution both locally and in other countries in Sub – Saharan Africa?

16. What is the importance of establishing IT control and audit in the management ICT risk management plan?
17. What is the purpose of a periodic review of user access rights within the PFMS environment?

18. How can communication between the office responsible for the granting and withdrawal of system access rights and the rest of the user groups be improved within the PFMS environment?

19. What in your opinion is stopping the operationalisation of the ICT risk management initiatives within the PFMS environment?

20. What other ICT risk management issues would you wish to be included in this research?

End of Questionnaire
Appendix “D”  PFMS user Depth Interview Guide

PART A  (Respondent profile and job functions)

1. Which position level are you in?
   a. Management level
   b. Operational level

2. Which department are you responsible for?
   a. Internal Audit department
   b. Information Communication Technology department
   c. Information Communication Technology Security department
   d. Risk Management department
   e. Accounting department

Section B : Standards and Frameworks Implementation

3. How is the PFMS configured so as to be able to address issues pertaining to successful ICT risk management within the PFMS environment?

4. According to the ministry’s Strategic Plan for the period 2010 to 2014, the first risk assessment report was due in March 2010 but up to now no risk assessments have been undertaken on the PFMS.

What challenges is the ministry facing in this respect?
5. What efforts have been made in ascertaining that the risk profiles of the ministry’s partnering companies guarantees future services for the PFMS from these companies?

6. What challenges have been encountered in seeking Service Level Guarantees with the companies that the ministry signed Service Level Agreements for the PFMS with?

7. Both the National ICT Policy and the ministry’s Strategic Plan reflect that the ministry intentions to address issues pertaining to successful ICT risk management within the PFMS environment.

What challenges are being encountered at the operational level since only a few ICT risk management action plans have been crafted but not operationalised within the PFMS environment over the period 2010 to 2014?

8. Hardware and Software licensing are relatively expensive.

What is the ministry’s position with regard to providing all its PFMS ICT applications with legal of use?
9. Government alone cannot sustain running the PFMS especially during the systems’ teething stage.

What efforts have so far been made toward identifying alternative sources of funding?

.................................................................................................................................
.................................................................................................................................
.................................................................................................................................
.................................................................................................................................
.................................................................................................................................
.................................................................................................................................
.................................................................................................................................
.................................................................................................................................
.................................................................................................................................

10. What have been your experiences in terms of system abuse by staff as a result of the current access control rights initiatives?

.................................................................................................................................
.................................................................................................................................
.................................................................................................................................
.................................................................................................................................
.................................................................................................................................
.................................................................................................................................
.................................................................................................................................
.................................................................................................................................
.................................................................................................................................
.................................................................................................................................
.................................................................................................................................
.................................................................................................................................

End of Questionnaire
Figure 4.1 Current Organisational Structure

Ministry of Information Communication Technology Postal and Courier Services
Figure 4.2: Proposed Organisational Structure

Ministry of Information Communication Technology Postal and Courier Services