INFORMATION AND COMMUNICATION TECHNOLOGY SECURITY GOVERNANCE IN ZAMBIAN BANKS

By

LEMMY P. MWANZA

A dissertation submitted to the University of Zambia in partial fulfilment for the requirements of the degree of Master of Engineering in Information and Communication Technology (ICT) Security

THE UNIVERSITY OF ZAMBIA

LUSAKA

2020

COPYRIGHT DECLARATION

DECLARATION

I, **Lemmy Patrick. Mwanza** hereby truthfully declare that I am the sole author of this report and all its contents are my original work that has before not been presented at any learning institution for an award. I further acknowledge that similar work has been done but not the same as this. All the work of other persons used to complete this project has been duly acknowledged and properly-referenced.

Signed:…… **Date:……**

Supervisor's Name…….

Signature…… **Date……**

CERTIFICATE OF APPROVAL

This dissertation of **Lemmy Patrick Mwanza** is hereby approved as fulfilling the partial requirements of the award of the Degree of Master of Engineering in Information and Communications Technology Security by the University of Zambia.

Examiner 1..... Signature …… Date.....

Examiner 2..... Signature …… Date.....

Examiner 3..... Signature …… Date.....

Chairperson of the Board

of Examiners ……..... Signature …… Date.....

ABSTRACT

This research seeks to broaden and strengthen the holistic understanding of ICT and Security governance effectiveness by specifically examining how ICT and Security governance practices provide a structure for banks to ensure that IT investments support business objectives. ICT and Security governance is one of these concepts that suddenly emerged and became an important issue in the information technology area. To address this objective, we investigate the operations of the banks, analyze IT governance practices and design an ICT and Security governance model and Information Security Strategy model that aligns Information Technology and Information Security with the corporate governance of the banks. Corporate Governance is the type of governance system that covers the organization's operations holistically. Corporate governances are cascaded to ICT and Security governance that covers and aligns IT strategy to the corporate business objectives. Therefore, Control Objectives for business-related technologies (COBIT) is one of the frameworks that is used for the implementation of ICT and Security governance in organizations. ICT and Security governance has been implemented by several organizations globally with the view of aligning IT to business requirements so that the shareholders may realize benefits from the investments. Locally, the Bank of Zambia has directed all the banks to implement good corporate governance. The republic of Zambia has also directed and mandated all the parastatal companies to formalize the implementation of the COBIT framework. In 2015, the auditor general indicated that all parastatal ICT audits were based on COBIT framework. The results showed that banks were not compliant with the COBIT process (EDM,AP0 and MEA) and only 3 banks had an IT representatives in the Executive Management. The study also showed that levels of ICT governance were practiced in the banks. However, the banks should conduct a gap analysis and formalize the implementation of COBIT as an ICT governance framework . The banks should further align operation processes with COBIT framework and also elevate Information Technology and Information Security to have a representation on Executive Management.

Keywords: Bank, Governance, Strategy, Objectives and Procedures

DEDICATION

This work is dedicated to my lovely family. In particular, my wife Bessy Nkhata and our two children, Mayamiko. and Mufaro. All your sacrifice and hard work was not in vain.

ACKNOWLEDGEMENTS

I am highly grateful to my supervisor Dr. Eliya Dani Banda for his kind guidance and advice in the process of this work. He was so speedy in his responses to my queries and made this worthwhile experience. Keep up the good work Dr.

I further wish to register my sincere gratitude to my lecturers in the school Electrical and Electronics Engineering at UNZA namely; Dr. Lubobya, Dr. Shabani, Dr. Banda, Dr. Phiri, Dr. Sanga and Dr. Mwanaumo. Not forgetting the administrative staff at UNZA.

I am so grateful to my friend. Lubasi K. Musambo and his family for their constant support and encouragement that made this work possible. You have such a great heart.

To my children, Mayamiko and Mufaro, I know you may be too young to understand why your Daddy was always away from you at a certain point in time, but I am confident that one day you will grow to understand what your Daddy did, because he wanted to able to provide a better life and future for you.

I love you dearly.

To my precious wife Bessy, my love, I am at a loss for words to express my gratitude to you for your consistent love, support and care during this very trying academic period. I promise that you will reap the fruits of your hard work of love.

Lastly, but by no means the least, my heartfelt appreciation is extended to God for giving me this opportunity and the strength, health and, peace of mind to attend at the highest institution University of Zambia.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ABBREVIATIONS AND ACRONYMS

AFIL	Agriculture Finance Company Limited
APO	Align, Plan and Organise
ATM	Automatic teller Machines
BAI	Build, Acquire and Implement
BAZ	Bankers Association of Zambia
BOZ	Bank of Zambia
CEO	Chief Executive Officer
CIO	Chief Information Officer
CISM	Certified Information Security Manager
CISO	Chief Information Security Officer
CISSP	Certified Information Systems Security Professional
COBIT	Control objectives for Information Related Technologies
COO	Chief Operations Officer
COZ	Credit Organization of Zambia
CRO	Chief Risk Officer
DDACC	Direct Debit and Credit Clearing
DSS	Deliver, Service and Support
EDM	Evaluate, Direct and Monitor
EFT	Electronic Funds Transfer
GRZ	Republic Government of Zambia
ICT	Information Communication Technology
Investrust	Investment Bank
ISACA	Information Systems Audit and Control Association
ISO	Information Standard Organization
IT	Information Technology
ITGI	Information Technology Governance Institute
MD	Managing director
MEA	Monitor, Evaluate and Assess
NATSAVE	National Savings Bank
NBFI	Non-Bank Financial Institutions
POS	Point of service
RTGS	Real Time Gross Services
SC	Stealing Committee
SIDO	Small Industries Development Organization
Stanbic	Standard Bank
Stanchart	Standard Chartered Bank
SWIFT	Society for the Worldwide Interbank Financial Telecommunication
TOGAF	The Open Group Architectural Framework
VPN	Virtual Private Network

WAN	Wider Area Network
ZANACO	Zambia National Commercial Banks
ZECH	Zambia Electronic Clearing House
ZISC	Zambia State Insurance Corporation
ZNBS	Zambia National Building Society
ZNPF	Zambia National Provident Fund

Chapter One

INTRODUCTION

1.1 Background

The banking industry dates back as early as 2000 B.C. The first bank in the world was a Merchant bank that offered loans to farmers and traders (Richard Hildreth, 2001). Banks are financial institutions that provide financial services and form the largest financial institution in the economy. They accept deposits from people (individuals and firms) and lends money in form of loans to individuals and firms (M. Buckle's, 2012).

The first bank in Zambia was established in 1956 and it was called the Bank of Rhodesia and Nyasaland. The followed the liberalized of the financial sector from Southern Rhodesia through the establishment of Bank of Rhodesia and Nyasaland. The bank was equipped with the full powers of a conventional central Bank such as conducting monetary policy, banker to the government and commercial banks, manager of foreign exchange reserves (BAZ, 2017)). The bank was also empowered to lend to the territorial and the Federal governments up to a limit based on their expected revenues in that fiscal year. The Bank of Zambia was established to take over from the Bank of Northern Rhodesia on the 7th of August, 1964 although its Act was only passed in June, 1965. In the same year of 1965, the Bank started operations as the Central Bank of Zambia that falls under the Ministry of finance as a department (BoZ, 2017).

Before independence, 3 foreign commercial banks dominated the banking sector namely Standard Chartered Bank, Barclays Bank, and Grindlays Bank providing fringe competition (Kalima, 2001). After the Mulungushi reforms of 1968, the government embarked on establishing financial institutions rather than nationalizing the existing ones. In 1969, ZANACO a first national commercial bank was established (Zanaco, 2017). In the same year of 1969, the government also established Non-Bank Financial Institutions such as the Zambia National Building Society, the Zambia National Provident Fund (ZNPF) and the Zambia State Insurance Corporation (ZSIC).

As of 2019, Zambia had 17 registered banks and of these, 12 were locally incorporated subsidiaries of foreign banks, 2 were partially owned by the Government of the Republic of Zambia and 3 were locally owned (BoZ, 2017) (BaZ, 2016).

The banks are registered by the Bank of Zambia (Sikazwe, 2014). They accept deposits and provide short-to-long term loans to their customers' banks have been categorized as public and private banks (Taylor, 2016). The banks where the Republic of Zambia is the major shareholders of the bank such as Zambia National Commercial Bank (ZANACO), National Saving Bank (NATSAVE). Private sector banks are the type banks where the majority of shareholders are the individual locals or foreigners examples are Investment bank of Zambia (Investbank), Standard Chartered Bank (Stanbic) (Heffernam, 2005).

Development banks are the types of banks that provide medium and long-term capital for the purchase of machinery and equipment, for using the latest technology, or for expansion and modernization (Prizzon, 2018). In Zambia, the development bank of Zambia (DBZ) identifies the project and provides funding for such a project. The Development of Zambia is owned by the Republic of Zambia and the African development bank.

Corporative banks are the types of banks that are formed by the people who jointly put resources together to serve their common interest under the Co-operative Societies Act (Krishna, 2018) When a co-operative society engages itself in banking business it is called a Co-operative Bank. The society obtains a banking license from the Reserve Bank of Zambia (4, 1997). Any co-operative bank as a society is to function under the overall supervision of the Registrar, Co-operative Societies of the State and the finance and backing act of 2017.

The banks in Zambia have adopted Information Communication Technology (ICT) as a key enabler to continuously restructure their operations to achieve more cost-effective and efficient operations and thereby achieving sustainable competitive advantage (Dr.G.Tulasi Rao, T.Lokeswara Rao, 2015).

Banks in Zambia are using Information Communication Technology as the driver for product innovation and delivering services to the customers through branch network interconnections (Santha Vaithilingam, 2006). However, many banks have established secure communication with

their branches through the use of private networks, (Olof Hesselmark, 2003). Virtual private network (VPN) is the technology used to secure the channel communication between the Commercial Banks and the branches through the usage of the unsafe public network (Lammle, 2016).

Governance is defined as the rules that run the organization through policies, standards, and procedures (ISACA, 2015). Corporate governance is the process and structure used to direct and manage the business affairs of an institution to ensure its safety and soundness and enhance shareholder value (Gëzim TOSUNI, 2013). ICT Governance is set rules that run the organization through policies, standards and procedures that effectively manage external legal, regulatory and contractual compliance requirements relating to bank's use of information and technology are increasing, threatening value if breached (ISACA, 2012). A policy is a deliberate system of principles to guide decisions and achieve rational outcomes. However, policies are implemented as a procedure or protocol. Policies are generally adopted by the Board of or senior governance body within an organization. Procedures are step by step sequence of activities on how to execute the policies. Procedures are developed and adopted by management (Hare, 2001). A standard is a repeatable, harmonized, agreed and documented the way of executing activities. Standards contain technical specifications or other precise criteria designed to be used consistently as rules.

ICT and Security governance practices once adopted and implemented may facilitate the IT-business strategic alignment and it might have an influence on the use of IT in an organization (Mwaulambo, 2017). The ICT and Security Governance Practices are defined as the arrangements and practices responsible for meeting the objectives and respecting the principles of IT Governance. ICT and Security governance is implemented using frameworks like COBIT. A framework is a real or conceptual structure intended to serve as a support or guide for the building of something that expands the structure into something useful. ICT governance Frameworks are types of frameworks that define–the ways and methods through which an organization can implement, manage and monitor ICT and Security governance within an organization (ISACA, 2012).

COBIT 5 is an ICT framework for governance and management of enterprise Information Technology (ICT) (CISM, 2015). COBIT stands for Control Objectives for Information Business Process, and it is the invention of a global task force and development team from ISACA, a

nonprofit, independent association of more than 140,000 governance, security, and risk and assurance professionals in 187 countries (ISACA, 2018).COBIT aims at delivering value through good governance and management of information and technology (IT) assets to the stakeholders. Enterprise boards, executives and management are the stakeholders that have to embrace IT as part of the business and maximize value from the investment (ISACA, 2012). COBIT is an effective tool for managing external legal, regulatory and contractual compliance requirements interrelated to enterprise use of information and technology. COBIT 5 standard provides a complete framework that supports enterprises to achieve their goals and deliver value through functioning governance and management of enterprise IT (George, 2014).

1.2 Statement of the Problem

Researchers have suggested that the adoption and implementation of ICT governance practices might be beneficial to the organization, because the organization may use its IT resources to achieve its business strategic goal (Weill & Ross, 2004). The organization with effective ICT governance may create business value and contribute to organizational performance growth (Weill, 2004). ICT and Security governance creates value for the business stakeholders and the organization implements it to influence the effectiveness of the organization's operations. Despite the beneficial role played by ICT governance practices in organizational performance, the adopted ICT governance practices and their influence on the effectiveness of ICT governance in the 17 Zambian banks are still not certain.

The ICT and Security governance model in an organization should meet its business requirements and operations. The field of ICT and Security governance is new and little research has been done for organizations in the financial sector to determine implementation of ICT and Security governance based on COBIT (Al Qassimi, 2015). Therefore, ICT governance model must be designed to meet the organization’s business objectives. Despite an increase in the use of ICT in the banks, little research in the field of ICT governance has been done in the financial sector. This has created a knowledge gap in understanding the insight on how IT aligns with business objectives. Therefore, Control Objectives for business-related technologies (COBIT) is one of the frameworks that is used for the implementation of ICT governance in Zambia and globally.

This study aimed to fill the noted knowledge gap by determining bank operation's organizational structure and the current level of ICT and Security governance practices in the bank. The study also aims to examine the implementation of ICT and security governance based on COBIT and design an appropriate model for the banks in Zambia. The proposed models determine the level of ICT and Security governance and recommend elevation of IT and Security to Executive management in the banks. The use of ICT has made the banking services to be delivered to the customers efficiently. ICT governance recognizes the importance of ICT and the need for ICT to driven by business interests (Paul A. Williams, 2015). ICT governance can be used to align the bank IT operations with the business corporate strategy and effectively improve the operations and management of the growing current problem of managing Information Technology.

Banks are among the organizations that have employed ICT applications to automate business process. ICT initiative established by the banks with the purpose to extend service delivery to the customers. ICT and Security governance has been implemented by several organizations globally with the view of aligning IT to business requirements. Locally, the Bank of Zambia has directed all the banks to implement good corporate governance. The republic of Zambia has also directed and mandated all the parastatal companies to formalize the implementation of COBIT framework (BOZ, 2016).

1.3 Objectives of the Study

The objectives of the study were to;

1.3.1 Investigate the operation structures of banks;

1.3.2 Analyze the usage of ICT in the Zambian financial sector;

1.3.3 Design a bank Structure Model to be adopted by the banks in Zambia based COBIT framework.

1.4 The Research Questions of the study

For this study the research questions were:

1.4.1 Establish the operating model for the banks in Zambia;

1.4.2 Determine applications of ICT in the financial sector;

1.4.3 Identify the ICT governance compliance levels with COBIT;

1.4.4 Examine the Implementation of ICT governance.

1.5 Significance of the Study

This study will give an improved method to the management of ICT and Security Governance in the financial sector in Zambia by employing ICT Governance so that shareholders realize the return on investment

1.6 Scope of the Research

This research study was limited to 17 banking institutions within the capital city of Lusaka as this is the headquarters for the banks. The study was further restricted to understanding ICT from a governance perspective.

1.7 Ethical Consideration

Due to the nature of the sensitivity of the data collected, the research study obtained ethical clearance from the University of Zambia's ethical guidance committee. All information collected was used primarily for academic purposes and the research participants were assured that their data would be used for the intended academic purpose only.

1.8 Organization of Dissertation

This dissertation is organized as follows;

Chapter 1 introduces this work and establishes the need to undertake this study. Chapter 2 illustrates various literature that has been studied to guide the research into a meaningful conclusion. Chapter 3 discusses the methodology undertaken in the research. Chapter 4 highlights the research findings and finally, Chapter 5 presents this study's conclusion, Recommendation and Limitations and Future Work.

Chapter 2

LITERATURE REVIEW

2.1 History of Banking In The World

Early 2000 B.C. Babylonians established the system of banking through their temples as banks (RHildreth, 2001). The new testament money changers are traces of banking. In ancient Rome also, banking was formed on lines of the Greek system (Vaish, 1991 and Anil Gupta, 1998). The evolution of banking is traced back to the 12th Century A.D in Venice and Geneva. The word 'banking' is believed to have originated from the German word (Richard Hildreth, 2001) meaning 'a mound or heap of money' (Parameswaran and Natarajan, 2001) which was Italianised into "Banco" (Richard Hildreth, 2001). The word "Bank" believed to be derived from the French word 'Banque' which means a 'Bench' where the business is transacted (Ajit Singh, 1986; Parameswaran and Natarajan, 2001). Thus, it is understood that there is no unanimity among economists about the origin of the word 'Banking' (Vaish, 1991). The first bank in the world was a Merchant bank that offered loans to farmers and traders (Richard Hildreth, 2001).

The word bank is rooted in the Latin meaning "bench" and refers to the orchestra in any Roman forum where money lenders used to transact (Vaish, 1991) Moneylenders who could be bankrupted if their loans went bad. The ancient and modern bankers relied on the assurance of the public to trust in their ability to choose good credit risk ratings from the bad. The borrowers deposited money in return for using the lenders' money with interest (Gupta, 1998). The subsequent credit crunches that resulted in the collapse of that trust and assurance are as ancient as credit itself.

The bank has turned the money from liability on one side of its balance sheet into a credit on the other side, such as a loan or bond to a business (Citibank 1994). The loan and bond, despite it representing money owed to the bank, is counted as an asset and is given a real value on the balance sheet based on an assessment of the risk that it won't be paid back; the higher the risk, the lower the 'book' value of the asset (Marcus, 2001). The loan also offers new money to the bank in the form of interest, a small portion of which is paid to the depositors as a reward for their confidence in the bank. The rest is profit after the wages of the bankers are taken into account (IONESCU, 2012).

2.1.2 History of Banking In Zambia

A bank is defined as an institution that provides banking services such as accepting deposits and providing loans (Martínez, 2006). A banking system offers cash management services for customers, reporting the transactions of their accounts and portfolios, throughout the day. The banking system, should not only be easy to use, but it should also be able to meet the new challenges posed by the technology and any other internal and external forces.

Before 1964, three foreign commercial banks dominated the banking sector namely Standard Chartered Bank, Barclays Bank and Grindlays Bank providing fringe competition (Kalima, 2001). Barclays Bank was established in 1918, the Standard Chartered Bank established in 1906 and the Grindlays Bank established in 1956 (Brownbridge, 2000). The banks were established to serve the mining sector and not the indigenous people.

In 1965, the Government perceived the foreign banks as not serving the interest of the local population in need of small and medium scale financial services. The same year Government attempted to nationalize the foreign banks to service the local population but failed as the foreign banks threatened to withdraw their expatriate management (Martínez, 2006). At that time the Government did not have the expertise to manage commercial banks (Maimbo, 2002). As an alternative, the Government decided to establish its bank that would serve the interest of the indigenous people.

In 1969, Government established Zambia National Commercial Bank (ZANACO) to improve credit services in the Zambian economy. In the same year Government also established the Land Bank to provide credit to the small-scale farmers in the agriculture sector (Martínez, 2006). The Land Bank was later replaced with the Credit Organization of Zambia (COZ). However, the COZ became insolvent due to poor repayment rates and was replaced by the Agricultural Finance Company Limited (AFC). The Zambia Agricultural Development Bank (ZADB) to cater to the commercial farmers was also established by the Government (Kalima, 2001). In 1987, the two government institutions, the Agricultural Finance Company and the Zambia Agricultural Development Bank were merged to create Lima Bank (Mishkin, 2009).

In addition to the commercial banks, the Government in 1971 established a number of Non-Bank Financial Institutions (NBFIs), notably, the Zambia National Building Society (ZNBS), which was a merger of building societies in Zambia, the Zambia National Provident Fund (ZNPF) and the Zambia State Insurance Corporation (ZSIC) a merger of insurance companies (M. Buckle, 2011). These institutions provided long term mortgages, pension funds, and insurance covers. Other financial institutions the Governments established to serve the interest of citizens in early 1980, were the credit guarantee scheme by the Bank of Zambia as a means of encouraging financial institutions to expand more credit to small-scale industries, the Small Industries Development Organization (SIDO), Village Industries Service and the Small Enterprise Promotion Ltd (Mwenda, 2002).

The Commercial banks and NBFIs which were established immediately after independence were heavily regulated (in terms of credit allocation and interest rates) by the Bank of Zambia. The deposit rates were below the market value, they offered easy account opening procedures and were over 200 branches (Mwenda, 2002). Such regulations led to financial markets in Zambia to be characterized by financial repression. Overall, the Government involvement in the financial sector resulted in an inefficient and noncompetitive market, which inhibited the development of the private sector financial institutions and discouraging private savings (Kalima, 2001).

Interest rate controls, which, together with, high reserve requirements, deteriorating macroeconomic conditions, political interference, negative interest rate policies, and directed credit policies, depressed profit margins for banks and reduced returns on financial assets for savers (Brownbridge, 1998). Furthermore, an inefficient payment system, an inadequate legal framework, and weak accounting standards reduced the banking systems efficiency, especially its ability to perform its financial intermediation function. Because of the above reasons, few private banks entered the sector between 1970 and 1990.

Prudent financial reforms in the banking sector only took place in the 1990s when the Zambian economy was liberalized. Through the liberalization policy, the Banking and Financial Services Act of 1994 and the Bank of Zambia Act of 1996 were enacted (Chiumya, 2010). These pieces of

legislation distinguish banking business from financial institutions. Banking business involves receiving funds from the public by accepting demand, time and saving deposits or borrowing from the public or other banks, and using such funds in whole or in part for granting loans, advances and credit facilities and for investing funds by other means (M. Buckle, 2011). Financial institutions are institutions whose regular business consists of granting loans, advances and credit facilities, and investing funds by other means, and whose business is financed by own or borrowed funds or with funds not acquired by accepting or soliciting deposits from the public (Mishkin, 2009).

2.1.3 Structure of Banking In Zambia

The Zambian financial institution has been structured with various types of banks. The banks operate to meet the financial obligation of different categories of people engaged in agriculture, business, profession, etc. The below chart shows how the financial institution has been structured (Mian, 2003);

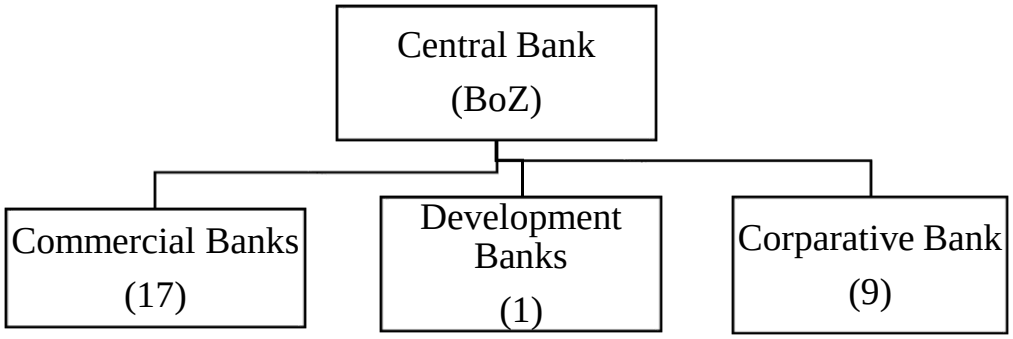

Figure 1 Bank structure

Central banks are defined as the highest bank that has been entrusted with the functions of guiding and regulating the banking system of a country (M. Buckle's Principles, 2012). Such a bank does not deal with the general public (Frederic, 2011). The central banks act essentially as Government's banker, maintain deposit accounts of all other banks and advances money to other banks when needed. The Central Bank guides other banks whenever they face any problem. It is therefore known as the banker's bank (Heffernam, 2005). The Bank of Zambia is the central bank of the Republic of Zambia. The Central Bank maintains a record of Government revenue and expenditure under various heads. It also advises the Government on monetary and credit policies and decides on the interest rates for bank deposits and bank loans (BAZ, 2017). Besides, foreign exchange rates are also determined by the central bank.

Commercial Banks are financial institutions that accept deposits and provides short-to- long term loans to their customers (M. Buckle, 2011). Commercial banks have been categorized as public and private banks. The public banks are the banks where the Republic of Zambia is the major shareholders of the bank such as Zambia National Commercial Bank (ZANACO), National Saving Bank (NATSAVE),. The private sector is the type banks where the majority of shareholders are the individual locals or foreigner's examples are Investment bank of Zambia (Investbank), Standard Chartered Bank (Stanbic).

Development banks are the types of banks that provide medium and long-term capital for the purchase of machinery and equipment, for using the latest technology, or for expansion and modernization (Prizzon, 2018). In Zambia, the development bank of Zambia (DBZ) identifies the project and provides funding for such a project. The Development of Zambia is owned by the Republic of Zambia and the African development bank.

Corporative banks are the types of banks that are formed by the people who jointly put resources together to serve their common interest under the Co-operative Societies (Krishna, 2018). When a co-operative society engages itself in banking business it is called a Co-operative Bank. The society obtains a banking license from the Reserve Bank of Zambia. Any co-operative bank as a society is

to function under the overall supervision of the Registrar, Co-operative Societies of the State and the finance and backing act of 2017 (Act, 2017).

2.2 The use of ICT in the Banking Sector

Information Technology (IT) is the automation of processes, controls, and information production using computers, telecommunications, software and ancillary equipment such as automated teller machine and debit cards (Alawode, 2011). It is a term that generally covers the harnessing of electronic technology for the information needs of a business at all levels. Communication is the conveyance or transmission of information from one point to another through a medium. Information is the customer details company details that are stored in computer system databases. Information Communication Technology is used as a tool and business enabler that allows the bank to deliver product and services to the customers (Anton, 2014).

Rapid advancement in ICT has had a profound impact on the banking sector and the wider financial sector over the last two decades and ICT has now become a tool that facilitates banks" organizational structures, business strategies, customer services, and other related functions (Dr.G.Tulasi Rao, 2015). Effective use of ICT is assisting banks to be more customers centric in their operations by building a more solid foundation in the customer relationship management system. ICT supports banks grow a range of products/services while mitigating fraud levels and improving risk management, broaden the customer base, reduce transaction and operational cost and also help gain a competitive advantage over competing banks (WESUTSA, 2010). The application of IT within banks is manifested through Networked branches, Automated teller machines, Point of Sale Banking, Mobile Banking, and Payment Transfers e.g. RTGS and SWIFT.

All the banks in Zambia are integrated into the Payment Settlement System. BoZ Central Securities Depository System Rules Jan-20160 observes that Real-time gross settlement systems are specialist funds transfer systems where the transfer of money or securities takes place from one bank to another on "real-time" and a "gross" basis (S M Kundishora, 2008). All Participants that are not classified as Bank shall appoint a Settlement Agent. Notification of the appointment of a Settlement Agent shall be made in Writing to BoZ by both the Participant and the Settlement Agent.

The banks in Zambia are using technology as the driver for the business (World,2013). Since 1996, the Bank of Zambia has been reaffirming the importance of having a well-functioning payment that

positively contributes to the financial stability of the country and the well-functioning of the country's economy (Payment, 2007). BoZ further states that a payment system is a system used to settle financial transactions through the transfer of monetary value and consist of the various mechanisms that facilitate the transfer of funds from one party (*the payer*) to another (*the payee*). Conversely, the Bank of Zambia realizes the important catalytic role that Digital Financial Services (DFS) can play towards the increased usage of electronic payment mechanisms by the general public (Matthew K. Luka, 2012).

The interest of network effect is significant in utilizing an Automated Teller Machines (ATMs) Kamyalile Simuchimba, BA (2011). Nevertheless, Milne also encourages and supports the notion (Milne,2006). Interestingly, further investigation Alhaji Abubakar Aliyu, Rosmaini Bin HJ Tasminon about the influence of the ICT evolution on the profit and cost-effectiveness of the banking industry (Alhaji, 2012). Further, a similar study in Kansas USA, by Sullivan also found no systematic evidence that multi-channel banks in the 10th Federal Reserve District were either helped or harmed by having transactional web sites (Muhammad, 2013).

The use of ICT in the banking industry enables global economies to set up a financial system before first establishing a fully functioning financial infrastructure. Electronic banking to be cheaper and reduces processing costs for providers and less search and switching costs for consumers, banks can promote their services and products involving transactions to all the income borrowers, even in remote areas (Shirley J. Ho, 2006).

The modernization of ICT sets the stage for extraordinary improvement in banking procedures throughout the world. For instance, the development of worldwide networks has considerably decreased the cost of global funds transfer (Alawode, 2011). Banks that are using ICT related products such as online banking, electronic payments, security investments, information exchanges, financial organizations can deliver high-quality customer service delivery to customers with less effort (Stella E. Igun, 2014).

2.3 ICT Technologies employed in the Banking Sector

Technology is a body of knowledge devoted to creating tools, processing actions and the extracting of materials. The term 'Technology" is wide, and everyone has their way of understanding its meaning. Technology is used to accomplish various tasks in our daily lives to solve problems that include transportation (drones), communication (fibre, microwave) and learning manufacturing. In the banking sector technology has been employed to delivery product and services to the customers (Alawode, 2011). The banks in the banking sector use ICT products to deliver services that include Automated Teller Machine, Smart Cards, Telephone Banking, MICR, Electronic Funds Transfer, Electronic Data Interchange, Electronic Home and Office Banking (Dr.G.Tulasi Rao, 2015).

The adoption and utilization of Information and Communication Technology (ICT) are fundamental to the growth and sustainability of the banking system. Since 1990 The Bank of Zambia and its Stakeholders have undertaken various initiatives to modernize the national Payment systems (KOSKOSAS, 2011). Innovation is a necessity for local and global competitiveness among the banks. As a result of globalization, the deployment of ICT in the banking sector has progressively become an essential influence for business development and a platform for gaining competitive advantage, especially in a highly competitive industry like banking (Reixach, 2001). This, therefore, made it necessary for banks to invest in ICT to meet certain requirements for a current payment system designed to process bulk transactions.

In 1999, the Bank of Zambia and its stakeholders established Zambia and electronic clearinghouse Limited (BoZ, 2004). The mandate of the establishing clearing house was to regulate the operations of the Payment Integration Gateway (PIC) and Direct Debit and Credit Clearing (DDACC) Payment Streams in line with the National Payment System Reform Programme and encourage the banking industry to take advantage of new business methods, technology (ZECH, 2014). In 2001, the Bank of Zambia and its stakeholders implemented Direct Debit and Credit Clearing (Payment, 2007). The banking sector has undergone reforms and in various ICT application has been deployed to enhance the banking operations are as follows:

2.3.1 Bank Connectivity

Banks in Zambia have established secure communication with their branches and other banks through the use of private networks (Esselaar, 2003). Virtual private networks (VPN) is the technology used to secure the channel communication between the Banks and the branches through the usage of the unsafe public network (Lammle, 2016). The banks have centralized the resources and the branches connect to the head office for resources using Virtual private networks (VPN) (Yadhu Ravinath, 2013). The bank branches are geographically scattered across the country and interconnected into one unified system located at the head office of the banks. This type of network is called Wide Area Network (WAN) and, through the WAN, branches are able to access customer information and products that enable them to deliver goods and services (Agboola, 2007).

2.3.2 Automated Teller Machine (ATM)

An ATM system is an electronic device that allows bank customers access their funds and be able to deposit funds without the intervention of bank staff (The Formal Design Model of an Automatic Teller Machine (Saadan, 2013) (ATM). Banks have deployed Automated Teller machines (ATM)s are systems deployed for easy accessibility of funds and also deposit by the bank account holders (Kamyalile, 2011). Bank customers are issued with the plastic smartcards (ATM Cards) and Identification Number (PIN). To access the funds, the bank account holders insets the Smartcard on the ATM slot and punches in the secret identification number on the ATM keypad (The Formal Design Model of an Automatic Teller Machine (Muhammad, 2013). ATM systems operate 24/7 and such security of the ATM systems and funds is critical for the banks. According to a survey conducted by PwC in Zambia, banks have been losing funds from cybercrimes (PwC 2018). Further, in the report, PwC observed that in 2017, 51% of the respondent indicated that they lost 51% of organizations reported having lost up to USD 100k (ZMW 954k) (PwC, 2018).

2.3.3 Mobile Banking

Mobile banking is defined as the technology that has revolutionized and changed the way banking is done (Sunil, 2015). Banks in Zambia have integrated banking systems with mobile network providers to enable the account holder to carry out transactions using mobile phones. Further Sunil Gupta, indicated that holders will have to use the Mobile USSD shortcode and the Mobile App i.e Zanaco *444# and the Xapit App. Mobile banking transaction has been less expensive as compared to traditional banking (Niina Mallat, 2004). Another research by Ph.D. Deepankar Roy, states that "Out of a world population of 7 billion, over 5 billion or 70% have a mobile phone, whereas only 2 billion or 30% have a bank account ". The paper further indicated that India has a population of 1.2 billion and of 1.2 billion, over 800 million have a mobile phone and only 250 million have a bank account (Pune, 2004) (Krugel, 2007).

2.3.4 Internet Banking

Internet banking is the type of banking where bank customers access funds over the Internet (Anton, 2014). This type of banking has attracted growing attention from bankers and other financial services players in the industry. Internet banking rapidly replacing the traditional brick and Mortar (FIRDOUS, 2017). The proliferating of electronic commerce is projected to cut banks' costs, increase banks' revenue growth, and make banking more convenient for customers; and some vexing public policy issues. Internet banking also enables customers to carry out certain transactions on their accounts with stringent security checks. Internet banking is described as the provision of traditional banking services over the internet (Journal (Alshammari, 2010). Internet banking offers a more convenient and flexible type of banking where customers are absolute in control over their banking activities (Niaz, 2010). Internet banking has an impact on bank overall performance by influencing the nature of linking between banks and their customers. As an alternative delivery of traditional retail banking, internet banking has an impact on the productivity of electronic banking.

2.3.5 Point of Sale (POS)

The role importance of payment systems has been closely monitored and promoted by the banks in Zambia (Zambia, 2015). A payment terminal, also known as a point of sale terminal (POS),

Electronic Funds Transfer (EFTPOS) terminal, is defined as a device which interfaces with payment cards to make electronic funds transfers (Whitteker 2014). Conversely, Olugbade Adeoti & Kehinde Osotimehin describes a POS is a system that allows customers to transfer funds instantaneously from their bank accounts to merchant accounts when making purchases using a debit card (Adeoti, 2013). The use of POS increases banking productivity and bank customers use of POS service for payments of goods and services, hence reducing the handling of cheques and cash withdrawals for shopping the operation (Osotimehin, 2012). Like an ATM, a POS system employs the Smartcard (Debit Card) that is inserted on the terminal Machine (Kamyalile, BA 2011).

2.4. Governance in the Banking Sector

Governance is defined as the Establishment of policies, and continuous monitoring of their proper implementation, by the members of the governing body of an organization. It includes the mechanisms required to balance the powers of the members (with the associated accountability), and their primary duty of enhancing the prosperity and viability of the organization (C.L.Parmo, 2009). ICT and Security governance is a formal framework that provides a structure for organizations to ensure that IT investments support business objectives.

The board has not paid much attention to IT matters hence creating serious problems over the two decades, Information Technology has moved largely a support back-office to becoming the key enabler and enabler business (ITGI ,2008). IT is not only critical in its support of key business processes but also transformational to the business at large. In a study conducted by PwC, it was found that while most organizations worldwide identify the importance of ICT and Security governance and most do not have a holistic view that considers all its dimensions (ISACA, 2006). The concept of ICT and Security governance as the main framework encompassing a wide spectrum of provisions, including the measurement of benefits, has yet to emerge. The alignment IT to the business objectives needs to be placed at the highest as a rated driver and desired outcome of ICT and Security governance practices (Ettish, 2017). The importance of IT alignment to deliver sustainable business results, and feel ICT and Security governance is one of the best means to achieve this (Michael, 2016).

The focus of ICT governance initiatives is still very narrow by focusing mainly on risk and control (Ettish, 2017). The initiatives are not considering ICT governance from a holistic perspective that can be used to enhance the value of IT for the organization. Without proper ICT and Security governance in banks, ICT systems can lose integrity with serious implications on the performance of a bank and can also result in a breach of client confidentiality (Rao, 2015).

ICT and Security governance is a new field and many organizations, governing information technology are finding it confusing to integrate IT with the company's overall corporate governance KPMG, 2004). It is further noted that discussions on the subject often are disjointed, laced with technical jargon, which only serves to confuse the very people who need to understand how to govern Information Systems(IS). Good management of IT results in the business value and alignment to the business goals. Corporate Governance in the banking system has assumed heightened importance and has become an issue of global concern because it is required to lead to enhanced services and deepening of financial intermediation on the part of the banks and enables proper management of the operations of banks (ITGI, 2003). The two main goals that include the ability of IT to deliver value to the business, which is driven by the strategic alignment of IT with business and the mitigation of IT risks, which is driven by embedding accountability into the enterprise (Michael, 2016).

Most banks knowingly or unknowingly practice ICT and Security governance. ICT and Security governance framework would enable a bank to perform its business in an orderly and effective manner benefiting the customers and, in the process, aid in its survival and growth (Sekar, 2010). The success of the banking business increasingly tends to hinge on the proper adoption and utilization of technology, but lately, ICT governance has assumed great significance. However, the frameworks, best practices, and standards are beneficial when they are adopted and applied effectively. With the current emphasis on the US Sarbanes-Oxley Act of 2002 and similar regulatory requirements related to enterprise governance and control around the world are significant so that ICT and Security governance and control are well understood, well positioned and well applied in the context of overall governance and control (Institute, 2005).

2.5 Corporate Governance in the Banking Sector

Corporate governance is the system of rules, practices, and processes by which a firm is directed and controlled. Corporate governance essentially involves balancing the interests of a company's many stakeholders, such as shareholders, senior management executives, customers, suppliers, financiers, the government, and the community. A typical organization has corporate governance, ICT and governance, and IT management. ICT and Security governance focuses on the IT-related areas within an enterprise corporate governance framework (Kan, 2003). Governance is a set of responsibilities and practices exercised by the board and executive management to provide strategic direction, ensure that objectives are achieved while evaluating the risks applying appropriate controls and verifying that the enterprise's resources are utilized effectively. The terms „governance", „enterprise governance" and ICT and security governance" may have different meanings to different individuals and enterprises depending on (amongst others) the organizational context (maturity, industry and regulatory environment) or the individual context (job role, education) (ITGI, 2009).

COBIT 5 proposes using the EDM02 to ensure the benefits delivery process to look at how best to optimize the value contribution to the enterprise from the business processes, IT services and IT assets resulting from investments made by IT at acceptable costs. EDMO2 is an acronym of COBIT 5 process number 02 that stands for Evaluate Delivery and Monitory and number 02. EDM processes of Governance ensures that stakeholder needs, conditions, and options are evaluated to determine balanced, agreed-on enterprise objectives be achieved. EDM02 prioritizes decision-making and it monitors performance, compliance, and progress against the agreed direction and objectives. The table below outlines the EDM02 organizational structure for governance practice;

Table 1 Governance structure (Source, ISACA)

Key Governance Practice	Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Business Executives	Business Process Owners	Strategy Executive Committee	Steering (Programmes/Projects) Committee	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information Security Officer	Architecture Board	Enterprise Risk Committee	Head Human Resources	Compliance	Audit	Chief Information Officer	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
EDM02.01 Evaluate value optimisation.	A	R	R	C	R		R			C	C		C	C	C	C	C	R	C	C	C					
EDM02.02 Direct value optimisation.	A	R	R	C	R	I	R	I	I	I	I	I	I	I	I	I	I	R	C	I	I	I	I	I	I	I
EDM02.03 Monitor value optimisation.	A	R	R	C	R		R			R	C	C	C	C	C	C	C	R	C	C	C					

2.5.1 Board of Directors

The Board of Directors ("the Board") is ultimately accountable for corporate governance as a whole. The management and control of Information Technology and Security is an essential part of corporate governance. In practice, however, the Board of Directors explicitly delegates executive responsibilities for most governance matters to the Executive Directors, led by the Chief Executive Officer (CEO) or Managing Director (Micheal Broudy, 2016).

The Board of Directors ("the Board") is ultimately accountable for corporate governance as a whole. The management and control of Information Technology and Security is an essential part of corporate governance. In practice, however, the Board of Directors explicitly delegates executive responsibilities for most governance matters to the Executive Directors, led by the Chief Executive Officer (CEO) or Managing Director (Micheal Broudy, 2016).

2.5.2 Executive Directors

The Executive Directors give overall strategic direction by approving and directing the Information Technology and Security principles and axioms but delegate operational responsibilities for Information Technology, Information and Physical Security to the Steering Committee (SC) (CLARKE, 2014). The Executive Directors depend heavily on the SC to coordinate activities throughout the organization, ensuring that suitable policies are in place to support the smooth running of the Information technology and security of the organization (C.L.Parmo, 2009). The Executive Directors also rely on feedback from the Steering Committee(SC), Chief Security Officer (CSO), auditors, Risk Management, Compliance, Legal and other functions to ensure that the principles, policies are being complied with in practice.

2.5.3 Chief Executive Directors

The Executive Directors demonstrate their commitment to the management of information technology and security through: A statement of support from the CEO; Reviewing and re-approving the principles and axioms every year; Approving the IT budget including a specific element set aside for information security; Receiving and acting appropriately on management reports concerning information security performance metrics, security incidents, investment requests (Bobbett R. Fagel, 2014).

2.5.4 Chief Information Officer

The Executive Directors have appointed a Chief Information Officer (CIO). The CIO is responsible for (Krishna Seeburn, 2014): Chairing the Information Technology Steering Committee; Planning Information Technology; Budgeting and Performance of Information Technology; Implementation of Information Technology and Security consistent with the policies and standards under the mandate of the CISO.

2.5.5 Chief Information Security Officer

The Executive Directors have appointed a Chief Information Security Officer (CISO). The CISO is responsible for (Bobbett R. Fagel, 2014): Chairing the Information Security Steering Committee; Taking the lead on information governance as a whole for instance by delivering the information security policy and providing the overall information security strategic direction, support, and review necessary to ensure that information assets are identified and suitably protected in the organization; Chief Security Officer further appoints and manages the Information Security Management team and the physical.

2.5.6 Chief Risk Officer

The Executive Directors have appointed a Chief Risk Officer (CRO). The CRO is responsible for (Micheal Broudy, 2016): Enterprise Risk Management. This includes the management of Information Security Risk and may also include noninformation risks such as operation risk, Environmental Risk and Credit Risk.

2.5.7 Chief Operations Officer

The Executive Directors have appointed a Chief Operation Officer (COO). The COO is responsible for (Bobbett R. Fagel, 2014); Oversee the day-to-day operations of the business of the organization; Develop, in association with the CEO and the Chief Financial Officer (the "CFO "), an annual operating plan that supports the organization’s long term operations strategy Assess and manage the principal risks of the organization's business within operations (proposals, projects, and staffing).

2.6 Information Security Governance

Information security governance is a subset of enterprise governance that provides strategic direction, ensures that objectives are accomplished, manages risks appropriately, uses organisational resources correctly, and monitors the success or failure of the enterprise security programme (Micheal Broudy, 2016). Information security deals with all aspects of information (spoken, written, printed, electronic or any other medium) and information handling (created,

viewed, transported, stored or destroyed). This is compared with IT security that is concerned with the security of information within the boundaries of the network infrastructure technology domain. (Bobbett R. Fagel, 2014)

Organisations today face a global innovation in governance that directly affects their information management practices. There is a heightened need to focus on the overall value of information protection from the intruders through the process called data loss protection (DLP) (Micheal Broudy, 2016). Due to the high-profile organisational failures of the past decade, legislatures, statutory authorities and regulators have created a complex array of new laws and regulations designed to force improvement in organisational governance, security, controls and transparency. Prior and new laws on information retention and privacy, coupled with significant threats of information systems disruptions from hackers, worms, viruses and terrorists, have resulted in a need for a governance approach to information management, protecting the organisation's most critical assets—its information and reputation (Harold F. Tipton, 2009).

Information and the systems that handle it are critical to the operation of virtually all organisations. Access to reliable information has become an indispensable component of conducting business; indeed, in a growing number of organisations, information is the business. Therefore, to achieve effectiveness and sustainability in today's complex, interconnected world, information security must be addressed at the highest levels of the organisation, not regarded as a technical speciality relegated to the IT department (Institute, 2005).

Information security is no longer a technical issue, but a business and governance challenge that encompasses adequate risk management, reporting and accountability. Effective security requires the active involvement of executives to assess emerging threats and the organisation's response to them (Bobbett R. Fagel, 2014). As organisations strive to remain competitive in the global economy, they respond to constant pressures to cut costs through automation, which often requires deploying more information systems. Whilst managers become ever more dependent on these systems, the systems have become vulnerable to a widening array of risks that can threaten the existence of the enterprise (Karen Scarfone, 2016). This combination is forcing management to face

difficult decisions about how to effectively address information security. This is in addition to scores of new and existing laws and regulations that demand compliance and higher levels of accountability.

The executive management has the responsibility to consider and respond to security concerns and while boards of directors will increasingly be expected to make information security an intrinsic part of the enterprise's governance efforts, aligned with their ICT governance focus and integrated with processes they have in place to govern other critical functions (CLARKE, 2014). Information security governance is the responsibility of the board of directors and senior executives. It must be an integral and transparent part of enterprise governance and be aligned with the IT governance framework. Whilst senior executives have the responsibility to consider and respond to the concerns and sensitivities raised by information security, boards of directors will increasingly be expected to make information security an intrinsic part of governance, integrated with processes they already have in place to govern other critical organisational resources (C.L.Parmo, 2009).

2.6.1 Protection of Information Assets

To exercise effective enterprise and information security governance, boards and senior executives must have a clear understanding of what to expect from their enterprise's information security programme. They need to know how to direct the implementation of an information security programme, how to evaluate their own status with regard to an existing security programme and how to decide the strategy and objectives of an effective security programme (Bobbett R. Fagel, 2014).

Data are the raw materials of information or unprocessed information. Data by themselves are useless until they are organized or manipulated in such a way that they provide information (Lammle, 2016). The information has been defined as data with meaning, relevance and purpose. Clearly, absent these attributes, there can be little justification for expending resources to protect it or, for that matter, retain it. Information is the basis for knowledge. Putting information together in such a way that it can be used to accomplish something useful is knowledge. Knowledge is created

from the information. Knowledge is, in turn, captured, transported and stored as organised information.

Information and the knowledge-based on it have increasingly become recognised as information assets, an example is a business-critical asset, without which most organisations would simply cease to function. It is a business enabler, requiring organisations to provide adequate protection for this vital resource (Harold F. Tipton, 2009). But to achieve effectiveness and sustainability in today's complex, interconnected world, security over information assets must be addressed at the highest levels of the organisation, not regarded as a technical speciality relegated to the IT department (Institute, 2005).

2.6.2 Benefits of Information Security Governance

Major international investors were willing to pay a premium for shares in an enterprise known to be well-governed. Further, investors pay more premium for companies where there is good information security governance. The demand for disclosure of the effectiveness of controls and attestation increased with the advent of financial reporting regulations and statutory requirements (BAZ, 2017). Information security governance is a firm foundation for efficient and effective risk management, process improvement, and rapid incident response related to securing information (McKinsey, 2003).

The benefits of good information security are not just a reduction in risk or a reduction in the impact should something go wrong. Good security can improve reputation, confidence and trust from others with whom business is conducted, and can even improve efficiency by avoiding wasted time and effort recovering from a security incident. Information also increases predictability and reduced uncertainty of business operations by lowering information security-related risks to definable and acceptable levels on security governance (Simonsson, 2008).

2.6.3 Importance Information Security Governance

A key goal of information security is to reduce adverse impacts on the organisation to an acceptable level of risk. Information security protects information assets against the risk of loss, operational discontinuity, misuse, unauthorised disclosure, inaccessibility and damage. It also protects against the ever-increasing potential for civil or legal liability that organisations face as a result of information inaccuracy and loss, or the absence of due care in its protection (Harold F. Tipton, 2009). Information security covers all information processes, physical and electronic, regardless of whether they involve people and technology or relationships with trading partners, customers and third parties. Information security addresses information protection, confidentiality, availability and integrity throughout the life cycle of the information and its use within the organisation.

Given the dramatic rise of information crimes, including phishing and other cyberattacks, few today would contend that improved security is not a requirement. With new worms/malware and the increase in reported losses of confidential customer information and intellectual property theft, senior management is left with little choice but to address these issues (Zambia, 2018). Information security requires a balance between sound management and applied technology. With the widespread use of networks, individuals and organisations are concerned with other risks pertaining to privacy of personal information and the organisation's need to protect the confidentiality of information, whilst encouraging electronic business (Lammle, 2016).

The systems and processes that handle information have become pervasive throughout enterprises. Organisations may survive the loss of other assets, including facilities, equipment and people, but few can continue with the loss of their critical information (i.e., accounting and financial reporting information and operations and process knowledge and information) or customer data (Yadhu Ravinath, 2013). The risks, benefits and opportunities these resources present have made information security governance a critical facet of overall governance.

Information security should be an integral part of enterprise governance, aligned with IT governance and integrated into strategy, concept, design, implementation and operation. Protecting

critical information must constitute one of the major risks to be considered in management strategies and should also be recognised as a crucial contributor to success (Harold F. Tipton, 2009).

2.6.4 Information Security Strategy

Information security governance requires senior management commitment, a security-aware culture, promotion of good security practices and compliance with the policy. It is easier to buy a solution than to change a culture, but even the most secure system will not achieve a significant degree of security if used by ill-informed, untrained, careless or indifferent personnel (N.C.Centre, 2005).

Information security is a top-down process requiring a comprehensive security strategy that is explicitly linked to the organisation's business processes and strategy. Security must address entire organisational processes, both physical and technical, from end to end. To ensure that all relevant elements of security are addressed in an organisational security strategy, several security standards have been developed to provide guidance and ensure comprehensiveness (Krishna Seeburn, 2014). Some of the most commonly used standards include Control Objectives for Information and related Technology (COBIT) and ISO 27001-201 (Bobbett R. Fagel, 2014).
A formal security strategy is implemented in part by developing and deploying comprehensive security policies that reflect the objectives of the organisation and address each element of the strategy. To provide effective governance, a set of enterprise standards for each policy must be developed to define boundaries for acceptable processes and procedures along with assigned roles and responsibilities (Craig A. Horne, 2015). Education, awareness and training must be provided to all personnel as part of an ongoing process to ensure that behaviours support secure, reliable operations.

A comprehensive security programme implements the protection of information assets through a layered series of technological and nontechnological safeguards and controls, example safety and environmental security measures, perimeter and physical security, background checks, access control security measures, user identifiers, passwords, IT technical measures and manual and

automated procedures) (Micheal Broudy, 2016). These safeguards and controls are necessary and should address threats and vulnerabilities in a manner that reduces potential impacts to a defined, acceptable level. Below shows an Information security governance layered strategy;

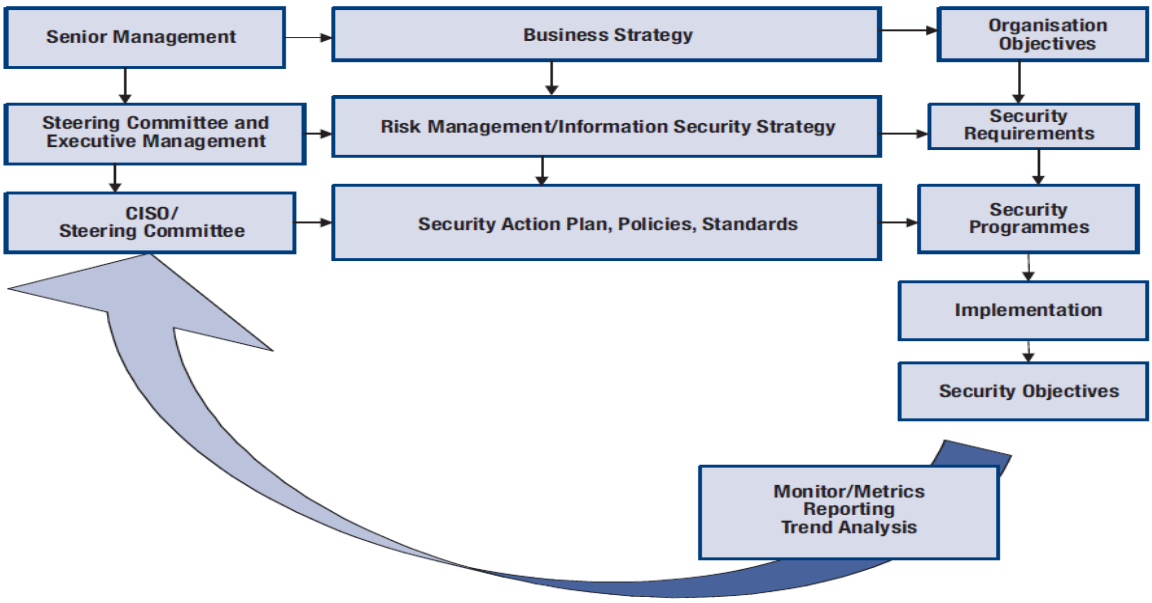

Figure 2 Information security governance layered strategy

The strategy provides the basis for an action plan comprised of one or more security programmes that, as implemented, achieve the security objectives. The strategy and action plans must contain provisions for monitoring as well as defined metrics to determine the level of success. This provides feedback to the chief information security officer (CISO) and steering committee to allow for mid-course correction and ensure that security initiatives are on track to meet defined objectives (MOHAMMED ALAA H. ALTEMIMI, 2015).

Once managers and directors know what information resources need what level of protection, information security baselines can be developed and implemented. Information security baselines are the minimum acceptable security that should be provided to protect information resources. Baselines vary depending on the sensitivity and criticality of the asset. Baselines can be expressed as technical, procedural and personnel standards throughout the enterprise (Max Shanahan, 2011). They are normally developed using a combination of accepted global standards such as COBIT, ISO 27001-2013.

2.7 IT Strategy in the Banking Sector

A strategy is defined as the direction an enterprise chooses to reach its goal. Goals are a description of the desired future condition, and strategy is the intentions of actions to realize the goals (N.C.Centre, 2005). The organisation strategy needs to consist of a set of main beliefs or formulas that are used to satisfy a company´s purpose (C.L.Parmo, 2009). These values are usually general directives for reaching some business goals. Strategies are plans that can be associated with project deployment and are defined from the overall business strategy, "Enterprise Architecture, IT Strategy and ICT governance (Orandi Mina Falsarella, 2017). An effective IT Strategy will benefit a company to achieve improved system solutions, from the upper management, precise resource estimations on IT-investments. An example IT Strategy covers the enterprise´s direction and strategy (mission, vision, goals, knowledge strategy), persons (competence needs), organization (future organization and control of the IT function), and an IT platform (computers, networks, databases, and applications) (CLARKE, 2014).

2.8 Banking Enterprise Architecture

The architecture defined as a structure and design of a system or a product and they also be defined it as the description of a set of components and the relationship between them (Sabine Buckl, 2010). In Information Technology (IT), Architecture has several branches: Software, Hardware, Systems, and Enterprise.

TOGAF open Group describes Enterprise Architecture as a still young discipline (TOGAF, 2012). Architecture progressed over the last 2 decade in terms of both its scope and its approaches and was established between the 1980s and 1990s as an approach for standardizing IT landscapes. Enterprise Architecture has become a critical tool for aligning an IT landscape to the requirements of the overall organization. Enterprise Architecture as the main components of an organization; its information systems, the ways in which the components work together to achieve defined business objectives and the way in which the information systems support the business processes of the organization (Ahsan, 2016). Enterprise architecting can be a set of processes, tools, and structures necessary to implement an enterprise-wide coherent and consistent IT architecture for supporting an enterprise’s business operations. (Jeff Tyree and Art Akerman, 2005) Enterprise Architecture as

a complete expression of the enterprise; a master plan which "acts as a collaboration force" between aspects of business planning such as goals, visions, strategies and governance principles.

Enterprise Architecture development is defined as planning for future state architecture, evaluating different scenarios and develop orientation points, processes and principles for the architecture (C.L.Parmo, 2009). Enterprise Architecture was discipline originally developed for organizing IT initiatives, but with the change in trends, it is now used trends for entire organizations from political, social, software, hardware and technology components (Maguire, 2017). Enterprise Architecture contains a framework and process. Enterprise Architecture framework as a set of best practice descriptions on how to execute the Enterprise Architecture process. Enterprise Architecture frameworks examples include; The Open Group Architecture Framework (TOGAF), the Federal Enterprise Architecture Framework (FEAF) and the Zachman Framework. Languages such as the Unified Modeling Language, ArchiMate and Business Process Model and Notation are described, as are Standards such as the National Information Exchange Model (NIEM) (Ramesh Radhakrishnan, 2004). Below are several reasons to organize an enterprise and implement Enterprise Architecture and important reasons include:

Alignment (how the enterprise is positioned and formed). Alignment between strategies, implementations and different sectors is crucial; Integrating operations and sectors; is essential in the semantic structures of the enterprise, the connectivity of the enterprise, and in the means of the enterprise and Promoting agility; the architecture must be built to handle change in technology and business objectives. Agility will also help reduce the time it takes to implement new solutions.

IT architecture is the organizing logic for data, applications, and IT infrastructure, captured in a set of policies, relationships, and technical choices to achieve desired business and technical standardization and integration (Sabine Buckl, 2010). By providing a road map for infrastructure and applications, architecture decisions are pivotal to effective IT management and use. Process integration allows multiple business units to provide a single face to a customer or to move from one important function to another.

Data refers to a collection of organized information; usually the result of experience, intelligence, observation or other important information within the enterprise. Applications refer to software

programs designed to perform a specific task or a group of tasks, such as word processing, communication or database management.

IT infrastructure is the foundation of planned IT capability (both technical and human) available throughout the business as shared and reliable services and used by multiple applications. Without a proper infrastructure, an enterprise may have limited sharing of resources, information, and expertise (Ramesh Radhakrishnan, 2004).

The various elements of the IT infrastructure may include Technology components (computers, printers, database software packages, operating systems, scanners); Telecommunication network services; Management of large scale computing (servers, mainframes); Management software (ERPs, customer relationship Management Systems); Management of shared customer databases; Research and development expertise aimed at identifying the usefulness of emerging technologies to the business; An enterprise-wide intranet. It is important to keep track of the company IT infrastructure to define possible extensions to meet the business process goals.

IT infrastructure, IT architecture, data, and applications are important concepts within Enterprise Architecture, but it is important to separate and have clear definitions of them when developing the Enterprise Architecture (EA) (Robertson, 2002). It is also important to state that classifying these concepts is only a small part of Enterprise Architecture.

2.9 COBIT Framework

COBIT 5 is a business framework for the governance and management of enterprise Information Technology (IT) (Pasquini, 2013). COBIT stands for Control Objectives for Information Business Process, and it is the invention of a global task force and development team from ISACA, a nonprofit, independent association of more than 140,000 governance, security, and risk and assurance professionals in 187 countries (ISACA, 2018).

COBIT aims at delivering value through good governance and management of information and technology (IT) assets to the stakeholders. Enterprise boards, executives and management are the stakeholders that have to embrace IT as part of the business and maximize value from the investment (ISACA, 2012). COBIT is an effective tool for managing external legal, regulatory and

contractual compliance requirements interrelated to enterprise use of information and technology. COBIT 5 standard provides a complete framework that supports enterprises to achieve their goals and deliver value through functioning governance and management of enterprise IT (George, 2014).

COBIT 5 processes are split into governance and management areas. However, the two (2) process areas contain a total of 5 domains and are called principles. The COBIT 5 domains are broken down into 37 processes (Krishna Seeburn, 2014). COBIT 5 provides a comprehensive framework that supports the organization in realizing its business objectives for the governance and management of IT systems (Vyas, 2016). COBIT 5 enables IT resources to be governed and managed holistically, taking in a full end to end business processes in an organization.

2.9.1 COBIT 5 PRINCIPLES

Governance and management of an enterprise information technology system is ultimately the responsibility of the board of directors' (or other leading entity's) (C.L.Parmo, 2009). The board sets the direction for management to realize the enterprise objectives and is answerable to the enterprise board of directors.

2.9.2 Principles 1. Meeting Stakeholder Need

The first principle looks at the need to align individual Information technology objectives with enterprise and organization stakeholder needs (Ettish, 2017). The purposes of ICT governance is to realize the strategic alignment of information technology objectives with the goals of the enterprise (Micheal Broudy, 2016). COBIT 5 constitutes the "top-down" entry point for enterprises that are considering the alignment of their information and related technology assets and resources.

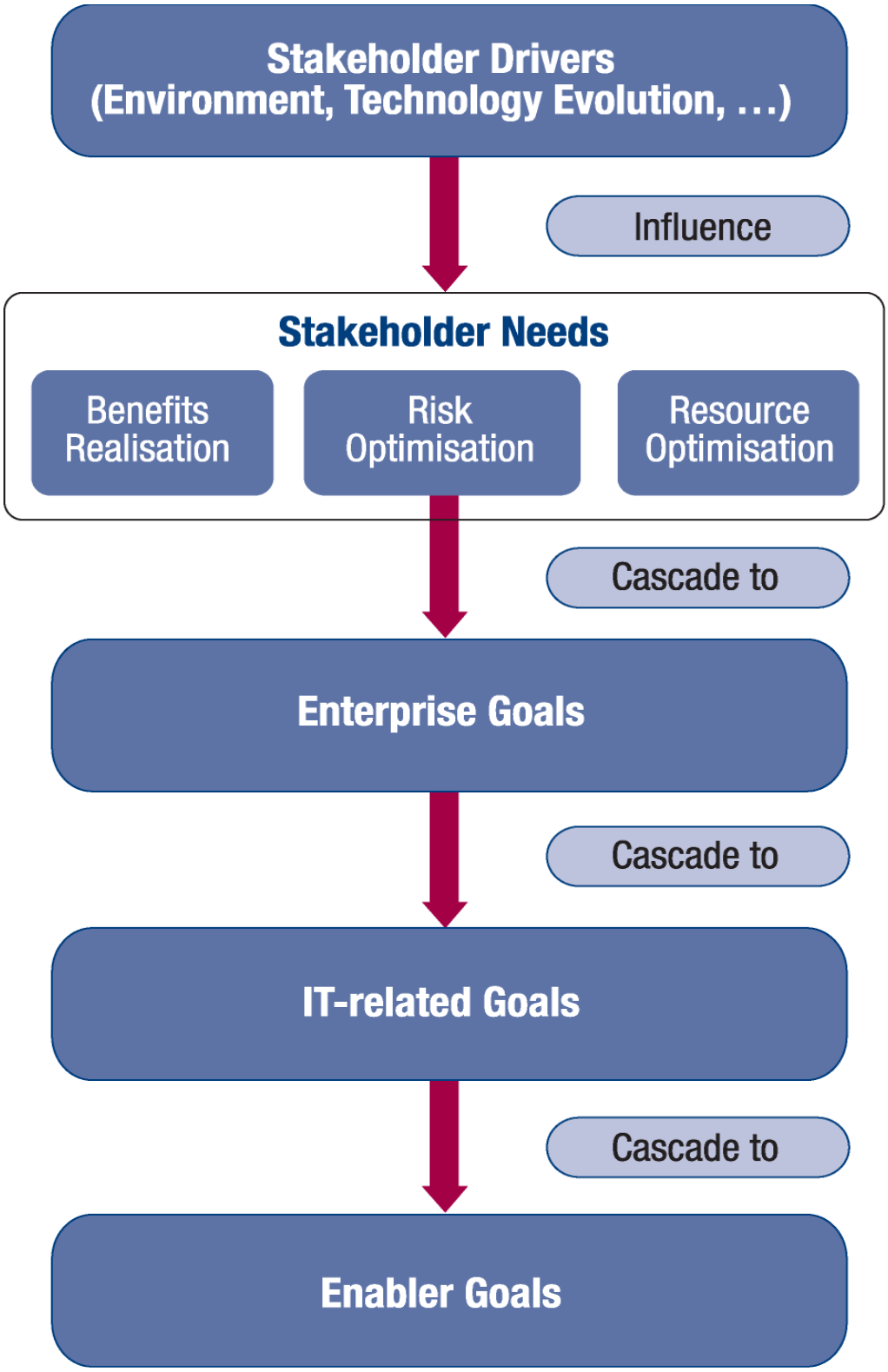

Figure 3 Technology Assets and Resources (ISACA, 2012)

2.9.3 Principles 2. Covering The Enterprise End-To-End

COBIT 5 covers all functions and processes in an organization, not just the IT department function, as was a case with earlier versions of COBIT. COBIT 5 considers information technologies to be assets and resources and takes them the same as other assets within the enterprise organization (Joanne De Vito De Palma, 2016). In COBIT 5, Business managers are mandated to take on the accountability for governing and managing the Information technology assets within their organizational units. Further, business managers must take ownership of, and be answerable for, governing the usage of IT while creating value from IT-enabled business investments—business managers must become more IT knowledge (Institute, 2005). COBIT offers a common, non-technical business language framework of control for business managers to use when engaging with their IT professional colleagues and advisors to make IT-related business decisions—supporting the IT environment (Pasquini, 2013).

Table 2 Covering the Enterprise end-to-end (ISACA, 2012)

	Business roles																IT Function roles								
AP001 RACI Chart																									
Key Management Practice	Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Business Executives	Business Process Owners	Strategy Executive Committee	Steering (Programmes/Projects) Committee	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information Security Officer	Architecture Board	Enterprise Risk Committee	Head Human Resources	Compliance	Audit	Chief Information Officer	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
APO01.01 Define the organisational structure.		C	C	C	C		I		C						R	I	I	A	C	C	C	R	C	C	C	
APO01.02 Establish roles and responsibilities.					I	C			C						C	C	C	A	C	C	C	R	C	C	C	C
APO01.03 Maintain the enablers of the management system.	C	A	C	R	C	C	I				C	C	C	C		C	C	R				R				
APO01.04 Communicate management objectives and direction.		A	R	R	R	I	R	I	I	I	R	R	I	I	I	I	I	R	I	I	I	I	I	I	I	I
APO01.05 Optimise the placement of the IT function.		C	C	C	C		A		C						C	C	C	R	C	C	C	R	C	C	C	
APO01.06 Define information (data) and system ownership.		I	I	C	A	R									C	C	C	C	C						C	C
APO01.07 Manage continual improvement of processes.				A		R			R				C		I	C	C	R	R	R	R	R	R	R	R	
APO01.08 Maintain compliance with policies and procedures.		A				R			R				R		R	C	I	R	R	R	R	R	R	R	R	

2.9.4 Principles 3. Applying A Single Integrated Framework

The third principle indicates the need to use an overall single, integrated ICT governance framework to deliver the optimum value from the IT assets and resources used (Micheal Broudy, 2016). However, COBIT 5 aligns with other relevant standards and frameworks such as ISO 27001 as shown ICT governance figure below;

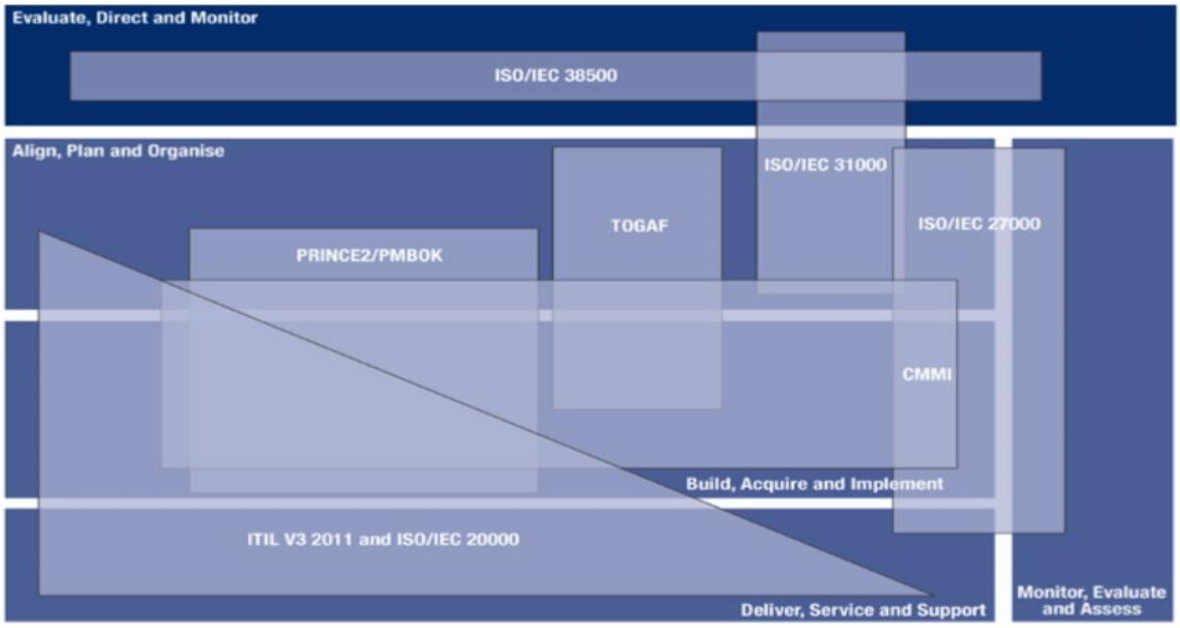

Figure 4 COBIT 5aligns with other framework (Krishna Seeburn, 2014)

The processes in COBIT 5 are inspired by the guidance in these standards and frameworks, that are used by IT professionals worldwide (Krishna Seeburn, 2014). The processes and practices in COBIT 5 aligned with more detailed standards or frameworks that are used by enterprises to govern and manage their IT assets and resources (Sona Karkoskova, 2016). COBIT 5 guides encompass high-level mappings of COBIT 5 processes to the major related standards and frameworks. COBIT 5 integrates and matches the Risk IT and IT framework guidance (Pasquini, 2013). COBIT 5 has been published into a single framework, making a "one-stop shop" for general GEIT guidance. COBIT 5 includes in its scope previous guidance from ISACA and guidance from other standards and frameworks in the field. Further, COBIT 5 provides a single overarching framework that serves as a consistent and integrated source of guidance in a nontechnical, technology-agnostic common language (CISM, 2014).

2.9.5 Principles 4 Enabling A Holistic Approach

The fourth principle stresses that efficient and effective implementation of ICT governance requires a holistic approach that takes into account several networking components or termed “enablers” in COBIT—because they interact to support governance and management of enterprise activities and are interdependent (Krishna Seeburn, 2014). The challenge of implementing a holistic approach is related to the need for an organizational system, which is; People, Processes, Technology, Culture, Infrastructure, Information and Policies and frameworks.

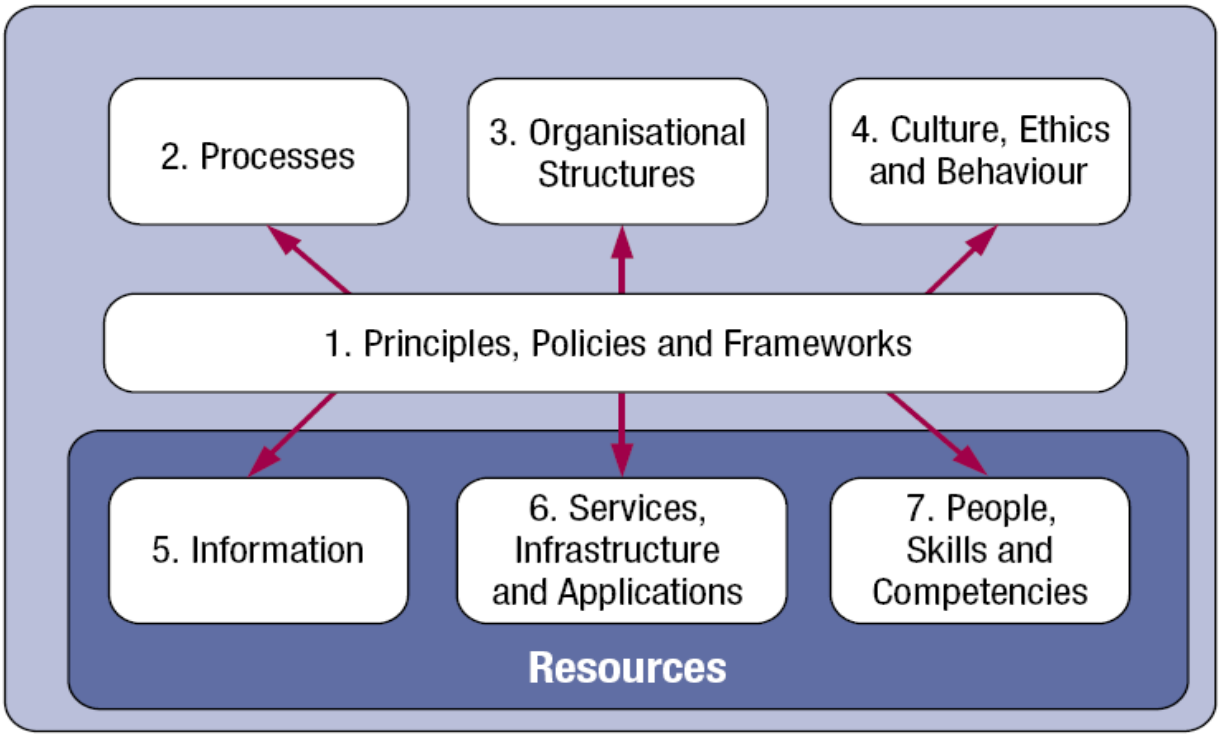

Figure 5 Enabling a Holistic Approach (Bobbett R. Fagel, 2014)

2.9.6 Principles 5 Separating Governance From Management

COBIT 5 final principle makes a distinction between governance and management. The distinction is aligned with the guidance in ISO/IEC 38500:2008:

The governance processes are arranged based on the evaluate, direct and monitor (EDM) model, as proposed by ISO/IEC 38500 (CIS (Krishna Seeburn, 2014). ICT governance processes ensure that

organizations goals are realized through evaluating stakeholder needs and setting organization direction through prioritization and decision making; and monitoring performance, compliance, and progress against plans (Mohanty, 2007). Based on the outcomes, guidance and output from these governance activities, business, and IT management strategies, builds, runs and monitors activities (PBRM) to ensure alignment with the direction that was set by the governing board of directors and, thus, accomplishing the enterprise objectives (Krishna Seeburn, 2014) figure below;

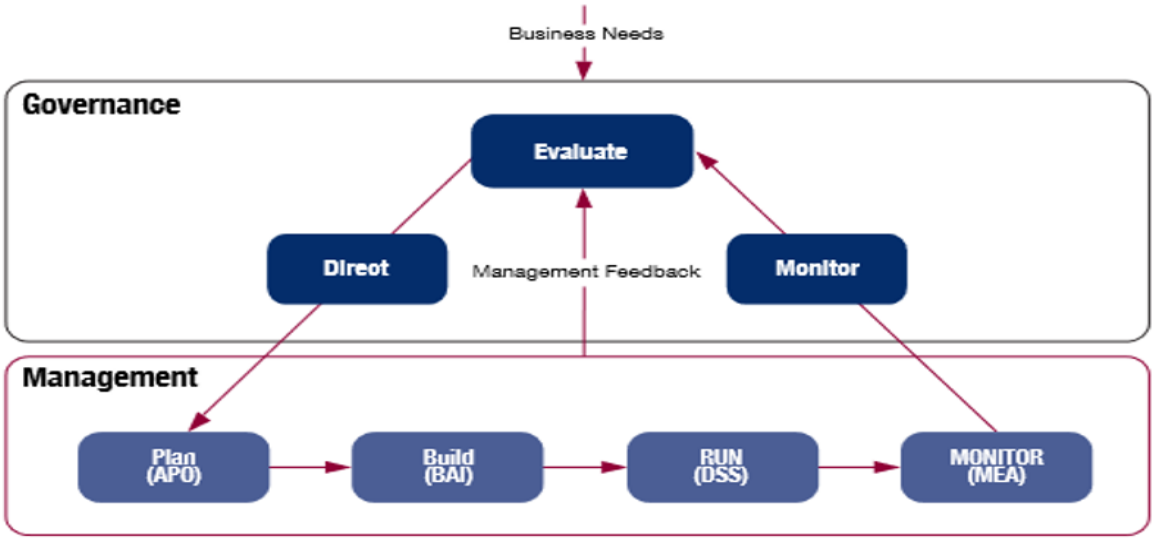

Figure 6 Separating Governance from Management (Debra Mallette, 2011)

COBIT uses maturity models called CMMI to measure the enterprise the progress against that goal. Additionally, the benchmark is used to compare their attributes to other companies within a specific industry (Pasquini, 2013). COBIT specific domain uses its maturity model for is ICT governance. More concrete the COBIT maturity model is measuring how well IT processes are managed.

2.10 ICT governance Implementation (COBIT)

COBIT 5 has been widely accepted as an ITG framework in various sectors of our economy. In Zambia, COBIT 5 has been implemented in both the public and private sectors. The companies where COBIT has been implemented include ZESCO, BOZ, ZANACO, and ZRA. (Report, 2015).

COBIT 5 has designed an implementation to help the institution in with the implementation process. The guide has broken down the implementation process into what is called seven phases of the implementation life cycle (Debra Mallette, 2011). The guide undergoes a frequent improvement of the life cycle to provides a method for enterprises to address the complexity and challenges typically encountered during ITG implementation (Karim, 2014). There are three interrelated dimensions to the life cycle, as illustrated in the figure below: the core ITG continual improvement life cycle, the enablement of change (addressing the behavioural and cultural aspects of the implementation or improvement), and the management of the Program. The three dimensions exist within each one of these phases. The seven phases of the implementation life cycle are illustrated in figure 7 below

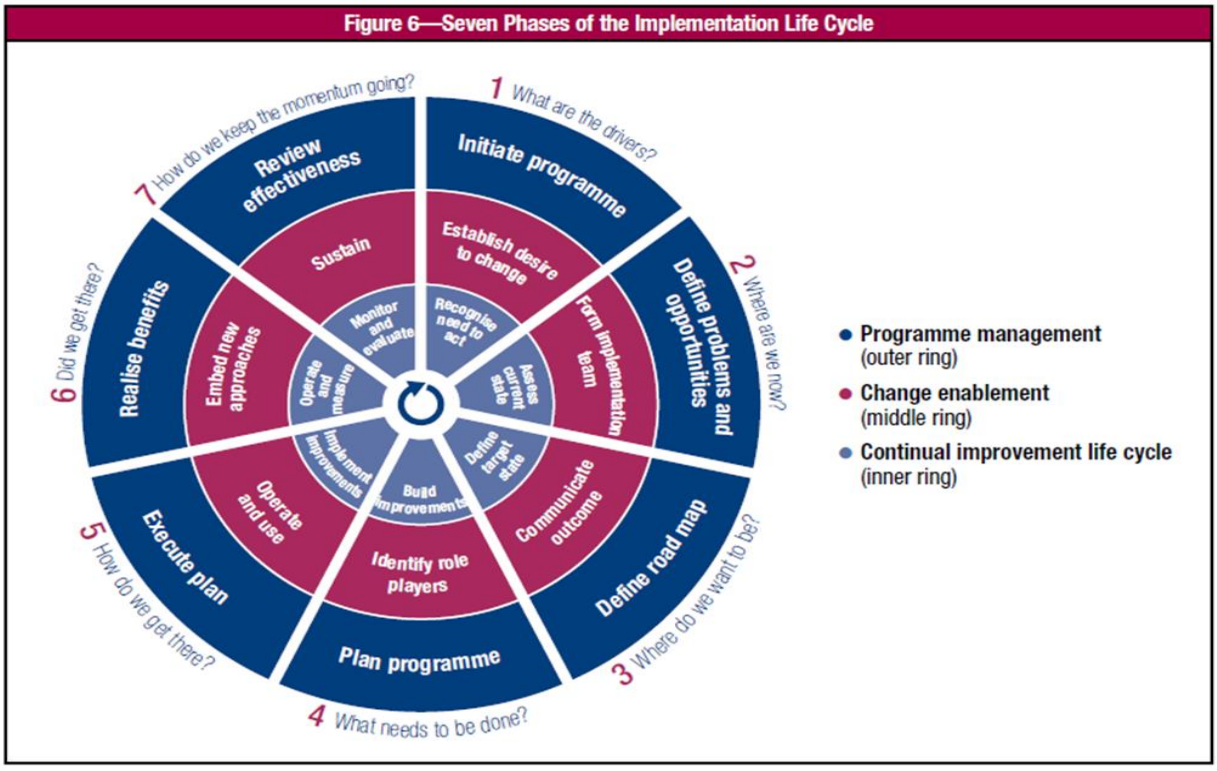

Figure 7 COBIT implementation phases (Debra Mallette, 2011)

2.10.1 Phase 1—What Are the Drivers?

Phase 1 Tries to recognize the current change drivers and creates at executive management levels a desire to change.

Key Questions, which need to be answered in this phase, include: What are the business motivation and justification for implementation? What are the Stakeholder requirements and expectations that should be fulfilled with COBIT? Why are we doing COBIT implementation?

There must be consensus on the need for implementing COBIT 5, to change and improve, supported by the will and commitment of executive management (Le Thanh Trung, 2013).

Dimensions: Program Management – Initiate the Program, Change Enablement – Establish the desire to change and Continual Improvement Lifecycle – Recognize the need to act.

2.10.2 Phase 2—Where Are We Now?

Phase 2 aligns IT objectives with organization enterprise strategies and risk, and priorities the most important enterprise goals, IT goals and processes. COBIT 5 delivers a generic mapping of enterprise goals to IT goals to IT processes to help with the selection. Management ought to know its current capability and where insufficiencies may exist. This is achieved by a process capability assessment of the as-is status of the selected processes (Karim, 2014).

Dimensions: Program Management – Define Problems and Opportunities, Change Enablement – Form the implementation team and Continual Improvement Lifecycle – Assess the current state

2.10.3 Phase 3—Where Do We Want To Be?

Phase 3 sets a target for improvement followed by a gap analysis to identify potential solutions. Some solutions will be quick wins and others more challenging, long-term tasks. Priority should be given to projects that are easier to achieve and likely to give the greatest benefit. Longer-term tasks should be broken down into manageable pieces (Vyas, 2016).

Dimensions: Program Management – Define the Roadmap, Change Enablement – Communicate outcome and Continual Improvement Lifecycle – Define target state.

2.10.4 Phase 4—What Needs To Be Done?

Phase 4 looks at feasible and practical solutions by focusing on critical projects supported by justifiable business cases. It develops a change plan for implementation. A well-developed business case will help ensure that the project's benefits are identified and continually monitored ((Pankaj Kumar Singh, 2014).

Dimensions: Program Management – Execute the plan, Change Enablement – Operate and use Continual Improvement Lifecycle – Implement improvements.

2.10.5 Phase 5—How Do We Get There?

Phase 5 delivers for the implementation of the proposed implementation plans through daily practices and the establishment of procedures and monitoring systems to ensure that business alignment is attained and performance can be measured (Paul A. Williams, 2015).

Dimensions: Program Management – Execute the plan, Change Enablement – Operate and Continual Improvement Lifecycle – Implement improvements.

2.10.6 Phase 6—Did We Get There?

Phase 6 Looks at supportable evolution of the enhanced governance and management practices into regular business processes and monitoring achievement of the enhancements using the performance metrics and anticipated benefits (Debra Mallette, 2011).

Dimensions: Program Management – Realize benefits, Change Enablement – Embed new approaches and Continual Improvement Lifecycle – Operate and measure.

2.10.7 Phase 7—How Do We Keep the Momentum Going?

Phase 7 evaluations of the overall accomplishment of the inventiveness, identifies governance or management requirements and strengthens the need for continual enhancement. It also priorities prospects to enhance GEIT (Le Thanh Trung, 2013).

Dimensions: Program Management – Review effectiveness and Change Enablement – Sustain

Continual Improvement Lifecycle – Monitor and The time spent per phase will change significantly depending on (amongst other factors) the specific enterprise environment, its maturity, and the

scope of the implementation or improvement initiative. However, the overall time spent on each iteration of the life cycle ideally should not exceed six months, with improvements applied progressively; otherwise, there is a risk of losing momentum, focus and buy-in from stakeholders (Sona Karkoskova, 2016).

Over time, the life cycle will be followed iteratively while building a sustainable approach. This becomes a normal business practice when the phases in the life cycle are everyday activities and continual improvement occurs naturally (Pasquini, 2013).

2.11 Challenges in ICT governance Implementation (COBIT)

Principles are the guiding procedures established to reinforce the implementation of good practices. ICT governance implementers should not overlook the COBIT 5 principles, which are pointers to the right way to implement ICT governance using COBIT 5 (George Mangalaraj, 2014). Adherence to the COBIT 5 principles can help an organization from missing the critical areas. The principles must govern the use of the business guiding framework. The first principle, Meeting Stakeholder Needs, is the major principle without which other principles become ineffectual.

The implementors should endeavour to get clarity on the business needs when implementing ICT governance. ICT governance through COBIT is about value creation, so the implementation must start with "why?". COBIT supports to balance benefit delivery with risk optimization and answerable use of resources such as people and systems (Ndlovu, 2016). Therefore, it is imperative to gain stakeholders' agreement on the stakeholders is receiving the benefits of ICT governance implementation, stakeholders are bearing the risk of the initiatives, and stakeholders are providing and managing the program resources (MOHAMMED ALAA H. ALTEMIMI, 2015).

The decision-making structure will influence the method used for ICT governance in the organization. The three most prevalent governance structures are centralized, decentralized and hybrid structures (John Dooney, 2016) . However, a suitable decision structure ought to be adopted by organizations as a critical success factor in ICT governance implementations. The focus on enterprise ICT governance and COBIT 5 places accountability with the senior management of a business, a centralized method would be most suitable as the senior management employ a focused

vision for the organization (Mohamed & Kaur, 2012). Stability is also necessary when implementing complex IT projects hence a centralized structure is appropriate

ICT governance implementation requires significant resources therefore appropriate budgetary control requirements to be exercised and resources made available (Onifade, 2018). The implementation of IT systems regularly brings about changes which impact on existing tasks and processes (1Karim Youssfi, 2014). The way that individuals understand the revolution to their business functions is as imperative as the actual change to the technology or business process itself. Consequently, an enterprise's approach to change management can have a greater impact on the success or failure of the ITG framework implementation or migration than the ability of the initiative to meet the business objectives for which it is intended (Kutzavitch, 2010).

Human Resource involvement in IT-related decision making and monitoring processes (Okon, 2017). It is very important for senior management to support and participation of stakeholders in ICT governance implementation. Implementation of IT also requires the engagement of other stakeholders (George Mangalaraj, 2014). Roles must clearly be well-defined and communicated with all stakeholders (C.L.Parmo, 2009). Studies have exposed the involvement of key stakeholders the more successful the governance of IT becomes (Nfuka, 2010).

IT resources and Governance training and awareness are required so that business processes are to be effective. Studies suggest that many businesses have difficulties related to budget limitations for IT resources and infrastructure enhancement (Maguire, 2017). Adequate investment is necessary to support appropriate infrastructure. Additionally, providing adequate awareness and training is principal and acts as a cornerstone to the development of an effective implementation strategy and subsequently to effective COBIT implementation

Chapter 3

METHODOLOGY

3.1 Research Design

The research was split between quantitative and qualitative research. Relevant published and unpublished materials aged less than 15 years were consulted in the study. The internet was a great resource, manly government sites, company websites in terms of Journal and publications and many more credible sites. Below is the figure that demonstrates the research methodology and the methods used in the research.

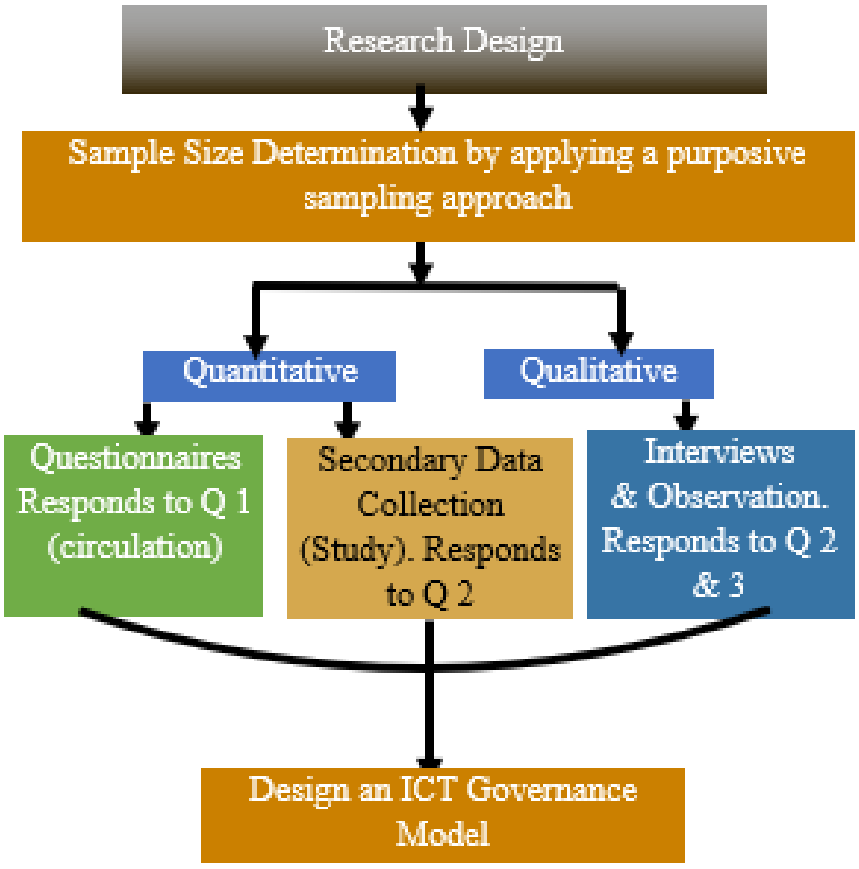

Figure 8 Research Design

The research design refers to the process that the investigator will follow from the inception to completion of the study area. The study used a descriptive study design. Descriptive research involves gathering data that describe events and then organizes, tabulates, depicts, and describes the data collected. This kind of design will allow data to be collected within the setting of the respondents and data analysis inductively construction from particular to general themes with the researcher interpreting the meanings of the data.

The questionnaire was grouped into four (4) sections consisting of eleven (11) questions in total. The first section, Section A, Bio Data - Please tick in the box as appropriate; Section B General Information (Please tick as appropriate); Section C, ICT governance issues; Section D challenges may have hindered successful adoption of appropriate ICT governance framework. Sixteen (17) commercial banks organizations with a sample size of 285 were targeted for the questionnaires with 39 respondents from 12 commercial banks responding.

A Likert scale was used to evaluate the level of agreement or disagreement with weights ranging from 1 - 5. This was used by respondents to evaluate the level of agreement or disagreement 5(100-80%),4(80-60%),3(60-40%),2(40-20%) and 1(20-0%) Percentages were used to find the level of agreement (sum of respondents for strongly agree and agree), disagreement (sum of respondents for strongly disagree and disagree), and neutral. The collected data were checked for completeness, and then coded, captured, and analyzed using Microsoft Excel. Descriptive statistics used included tables, frequencies, weighted mean, standard deviations, and percentages.

Before a face-to-face interview could be conducted, it had to be established that respondents were 1) familiar with infrastructure sharing issues and the notion of sharing and 2) knowledgeable of decision-making strategies used in infrastructure sharing by mobile operators or new entrants. The main reason for this was to minimize errors in data collection and derive valid information that is considered by the network operators, tower operators, and possibly the new entrants concerning infrastructure sharing to eventually compare them with our respective hypotheses based on literature findings.

Before contacting any potential respondents to be interviewed, the Human Resource departments in the respective organizations had confirmed thoroughly their positions and areas of involvement to be sure that they were relevant and met the sample selection criteria. All potential respondents

were then contacted through a phone call and advised of the purpose of the interview. Additionally, all of them received an introductory letter indicative of the questions that would be discussed in the interview. After the interview, questionnaires were left to be filled out by the other respondents in that organization.

Nine interviews in total were recorded. During the interviews, it was clearly stated to all the interviewees that anonymity would be kept, and their names would not be mentioned. The target population was the technical staff that usually work or are found in the field at a tower site; however, due to logistical challenges of reaching the respondents for interviews, questionnaires were administered. The interview questions are covered in Section B of the appendices.

One of the limitations of this study is that it is highly dependent on the technical people who have hands-on experience in the field. Less than twenty individuals at each targeted organization in this research could provide complete and valid information, and the researcher relied heavily on interviews as a backup method of collecting data from the heads of departments to confirm that the data collected from the respondents were valid. Having an alternative method for collecting empirical knowledge could be a way to overcome this limitation. Other limitations are related to the scope of this study.

3.2 Sample Size

Data was collected from 50 participants from the 17 commercial banks. The research targeted the population of 255 and the sample size of 37 participant's working in the IT department for various commercial banks. The study was also done through direct observation and interview visits to various commercial banks.

$$n_r = \frac{4pq}{d^2} \qquad \text{Eqn. 1}$$

Where;

n_r = required sample size,

p = proportion of the population having the characteristic,

q = $1 - p$ and

d = the degree of precision.

The proportion of the population (p) may be known from prior research or other sources; if it is unknown, use p = 0.5, which assumes maximum heterogeneity (i.e., a 50/50 split). The degree of precision (d) is the margin of error that is acceptable. Setting d = 0.1 0, for example, would give a margin of error of plus or minus 10%. Applying this formula to this research;

Since the researcher does not know, Gogtay (2010) recommends the researcher to assume = 0.5, and the value of q is = 1- p, d is to 90% accuracy; therefore

P = 0.5

Q = 0.5 and

d = 0.1, margin of error of ± 10%.

Therefore, the sample size is calculated with a confidence level of 90%, to be.

$$n_r = \frac{4pq}{d^2} \qquad \text{Eqn 2}$$

$$n_r = \frac{4 * (0.5) * (1 - 0.5)}{0.1^2}$$

The sample size is calculated with a confidence level of 90%, to $ben_r = 100$

3.3 Population

The study targeted all the 17 commercial banks in Zambia as of 2017 (BOZ, 2017). Further, the study targeted a population of 255 and a sample size of 37 participants working in the IT department for various commercial banks. The banks were chosen since they have led to the implementation of ICT.

3.4 Data Collection

The study used a semi-structured questionnaire for data collection and each bank was administered five questionnaires. Questionnaires had three sections; Section A was be used to collect profile and bank operations model data of the respondents and banks, section B focused on the five COBIT

ICT governance domains while section C helped collect data on challenges that may have hindered successful adoption of appropriate ICT governance framework.

Ethical issues procedures were involved to protect the respondents‟ confidentiality. First, the researcher ensured that the respondents did not write their names, personal or identification numbers on the questionnaires. Questionnaires were administered and collected in person from the participants. The researcher was able to handle sensitive and confidential issues as advised by the researcher.

3.5 Data Analysis

Collected data from the questionnaires were computed and tabulated. This was to facilitate analysis using descriptive statistics. The findings were presented using tables, frequencies, and percentages. This aided in presenting vital information on ICT governance Practices in Commercial Banks in Zambia.

Section A was analyzed through tables and percentages to depict a pattern. It covered information on demographics from the commercial banks covered in the study.

Section B helped understand ICT governance issues and COBIT. It involved analysis of the extent of adoption of ICT governance best practices by the commercial banks in Zambia through tables and percentages.

Section C covered the challenges that may have hindered the successful adoption of an appropriate ICT governance framework. The mean score and standard deviation were used to analyze and interpret the challenges hindering the successful adoption of an appropriate ICT governance framework by the commercial banks. Due to the quantitative nature of data gathered, Microsoft Excel tool for windows as the most suitable tool to analyze the data was used.

Chapter 4

DATA COLLECTION AND ANALYSIS

4.1 Study Respondents details

Classification of bank ownership and other findings are discussed in this chapter.

4.1.1 Ownership of the commercial bank

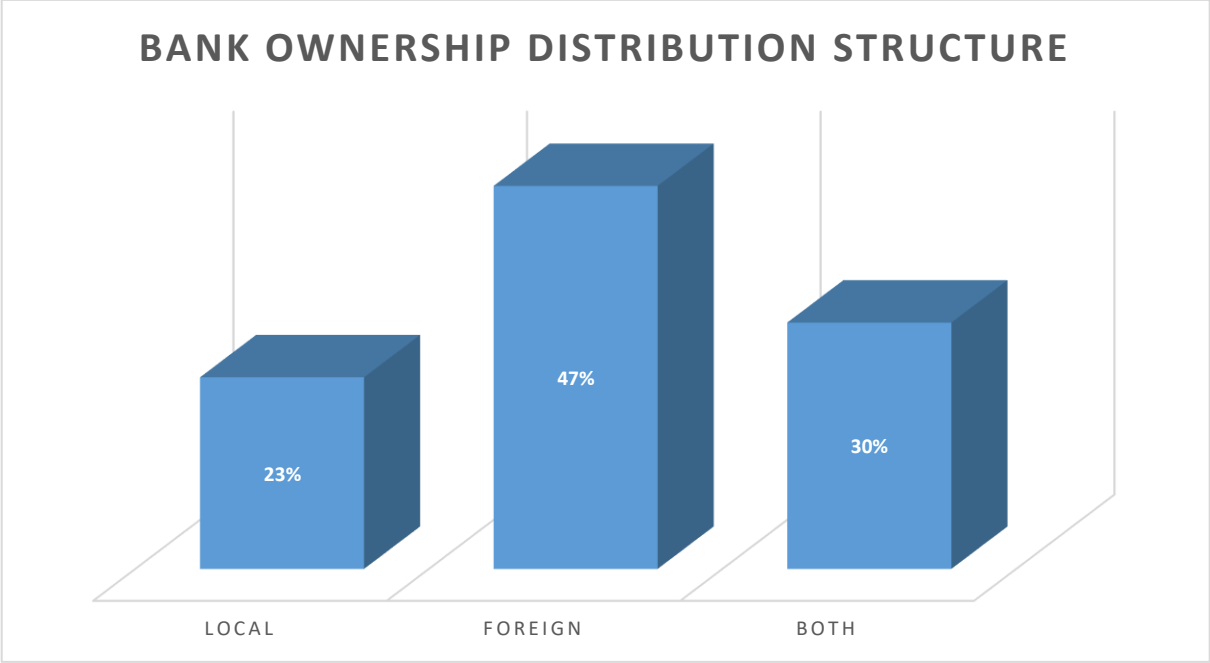

Figure 9 Distribution of respondents by bank ownership structure

The figure 9 above shows that the ownership of the banks, 23% of the respondent indicated that locals owned their bank, 47 % of the respondent indicated that foreigners owned their bank, and 30 % of the respondent indicated that the locals and foreigners owned their banks.

4.1.2 The Number of commercial bank branches

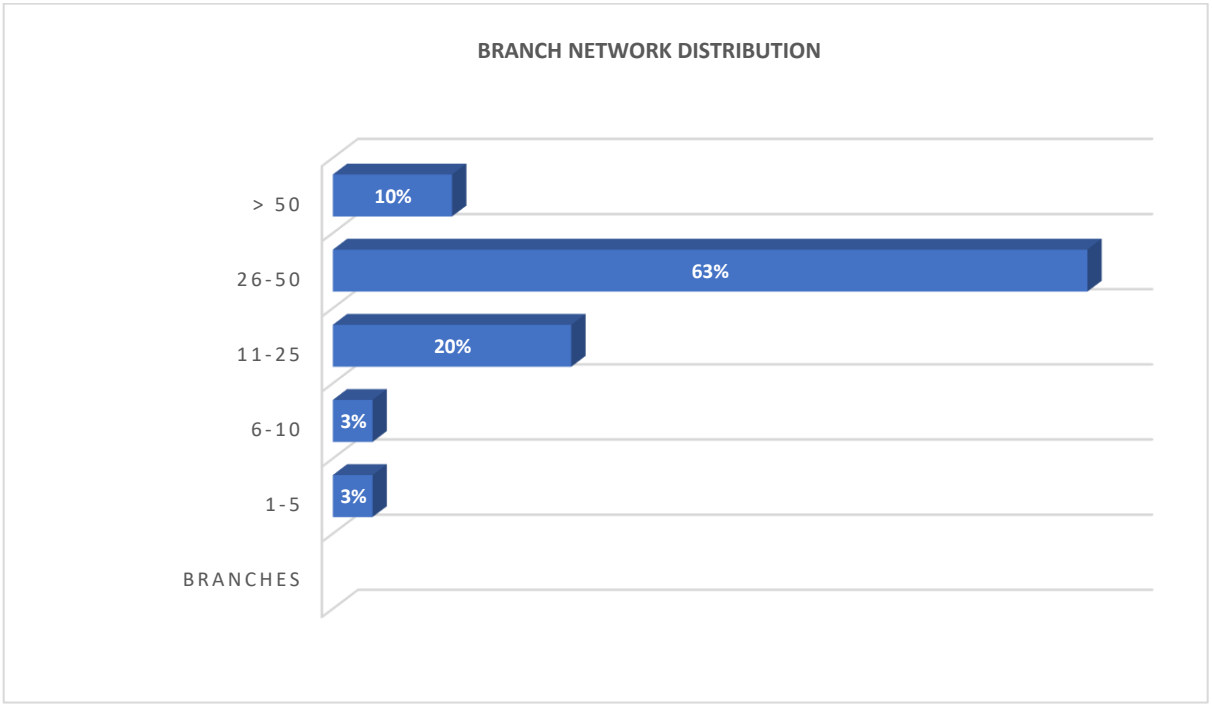

Figure 10 Distribution of Number of commercial bank branches

Figure 10 shows most of the respondents were from the banks that had between 26-50 local branches of a bank, with a response of 64%, between11-25 accounted for 20%, above 50 accounted 10%, between 6-11 that accounted for 3% and 3% for between 1-5 branches.

4.1.2 Years the Bank has been in Operation

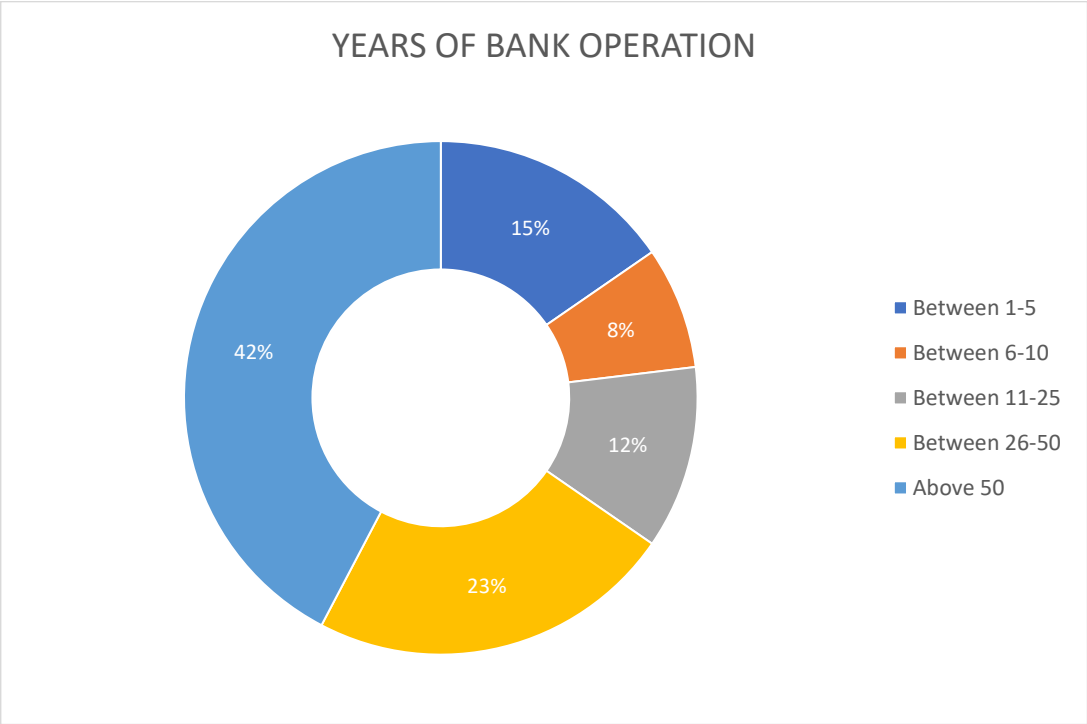

Figure 11 Years the Bank has been in Operation

Figure 11, majority (42%) of respondent's indicated the banks have been in operation for more than 50 years, 23% for between 26-50 years, 15% for between 1-5years, 12% for between 11-25years and 8% have operated between 6-10 years.

4.1.4 Designations Level of Respondents

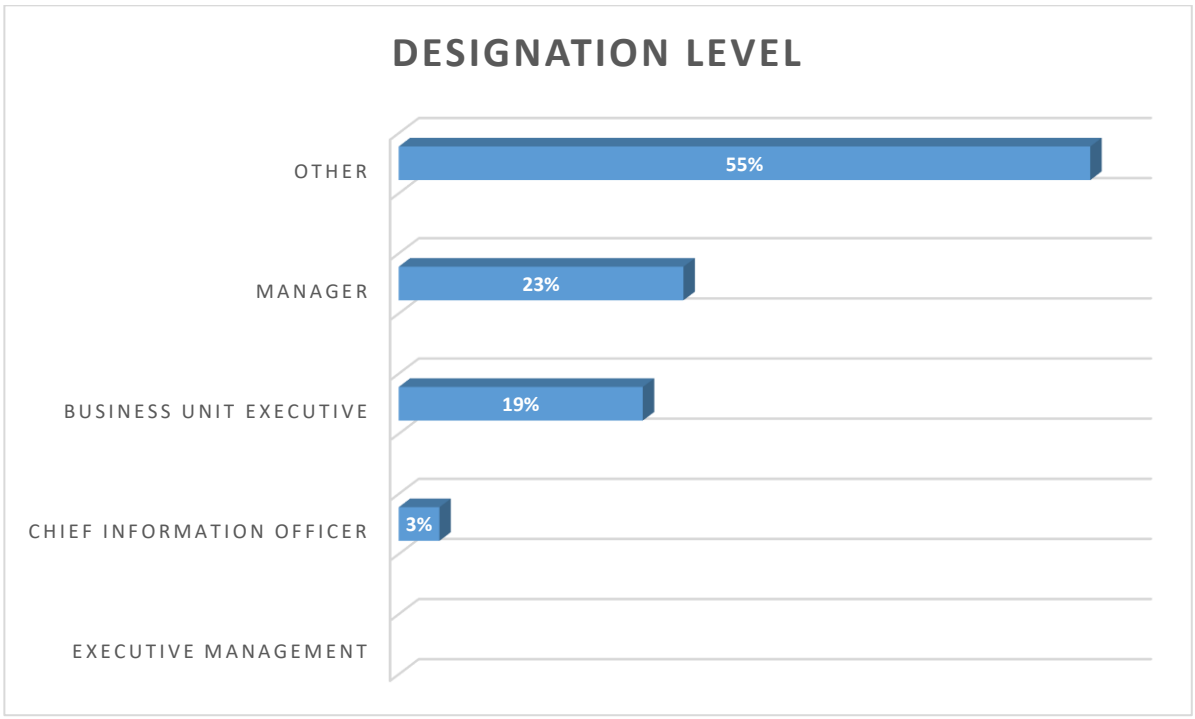

Figure 12 Designation Level of Respondents

From figure 12, the majority of respondents had the titles not specific to the listed and representing 55% of responses, 23% of the responders were Managers, 19% business unit executive or unit heads and least of the responders of 3% was Chief Information Officer.

4.1.5 The frequency of IT strategy Committee meeting

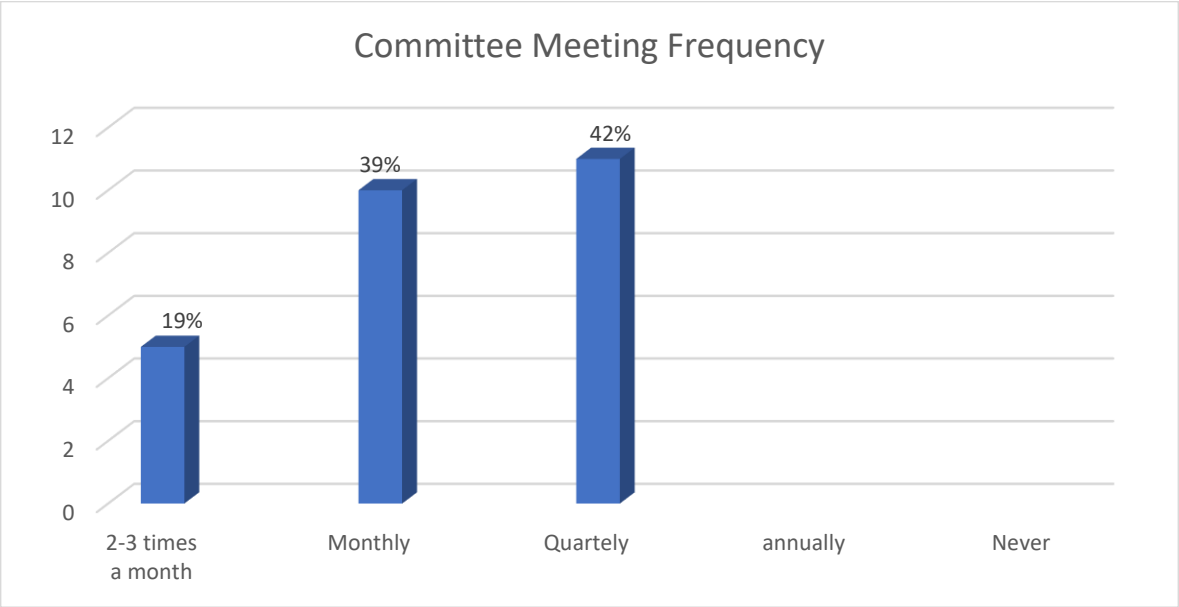

Figure 13 The Frequency of IT Strategy Committee Meeting

From figure 13, the majority of respondents (42%) agreed to the IT strategy committee meets quarterly, 39% responders indicated that the IT Strategy committee meets monthly and 19% of the responders indicated that they meet 2-3 times a month.

The research finding agreed with the publication of the ICT governance Institute in terms of the frequency the IT Strategy committee meets to discuss the review and discuss IT strategy. The respondent of the survey by ICT governance Institute (2005) indicated that 52% meets weekly, 37% meets Quarterly and 32% meets monthly. The respondent interviews also noted that the committee does not assume the Board of Directors role but its role is merely on advising ICT governance of the bank.

4.1.6 The board reviews of IT budgets and plans regularly

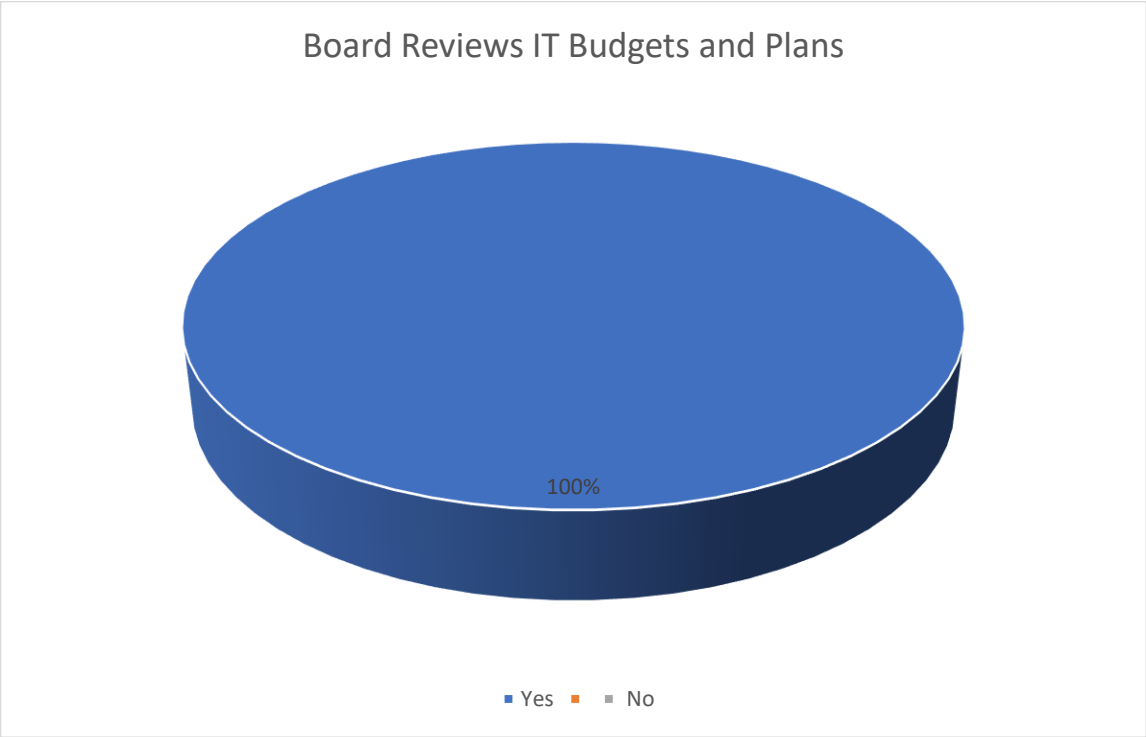

Figure 14 The board reviews of IT budgets and plans regularly

From figure 14, all respondents agreed that the board of directors reviews IT budgets and plans regularly.

4.1.7 Structured Processes for Good ICT governance

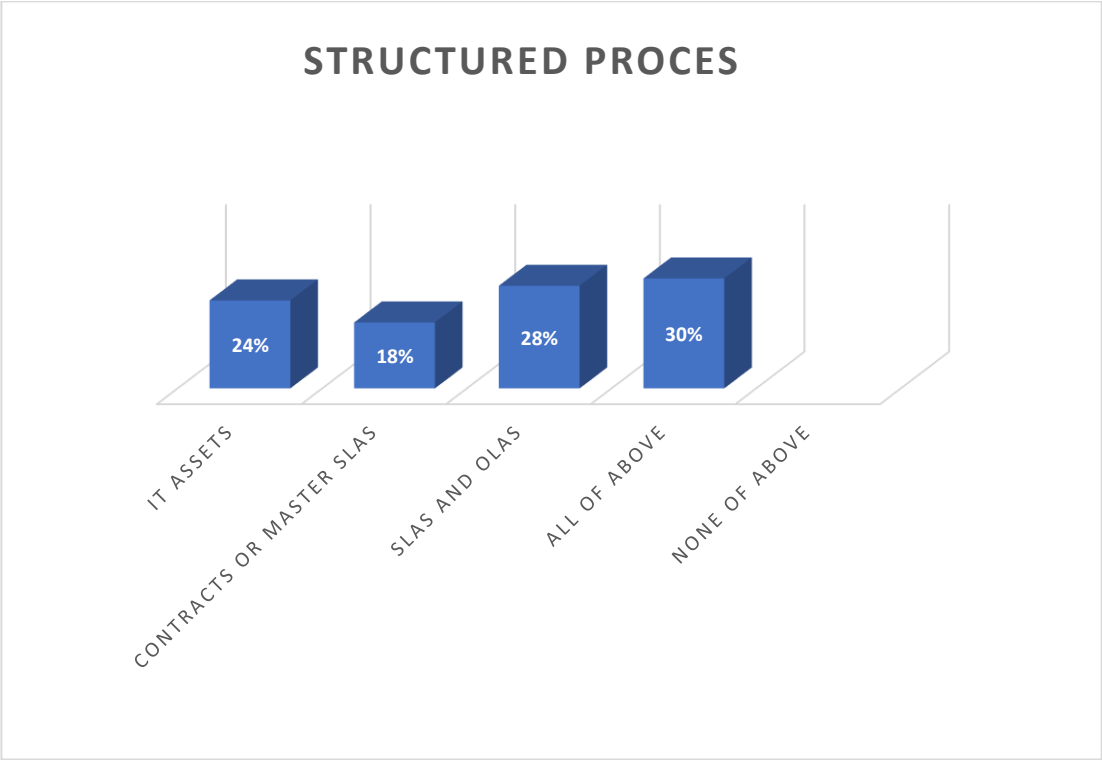

Figure 15 Structured Processes for Good ICT governance

Figure 15 shows that 30% of respondents indicated that the process of governance such as IT Assets, Contractors and Service Level Agreements (SLA) are used to govern the IT Systems and people in the commercial banks. Besides, 28% of respondents indicated that Service Level agreements are used to manage the outsourced services, 24% of respondents indicated that IT assets are classified

4.1.8 Standard IT Process Governance Frame Work

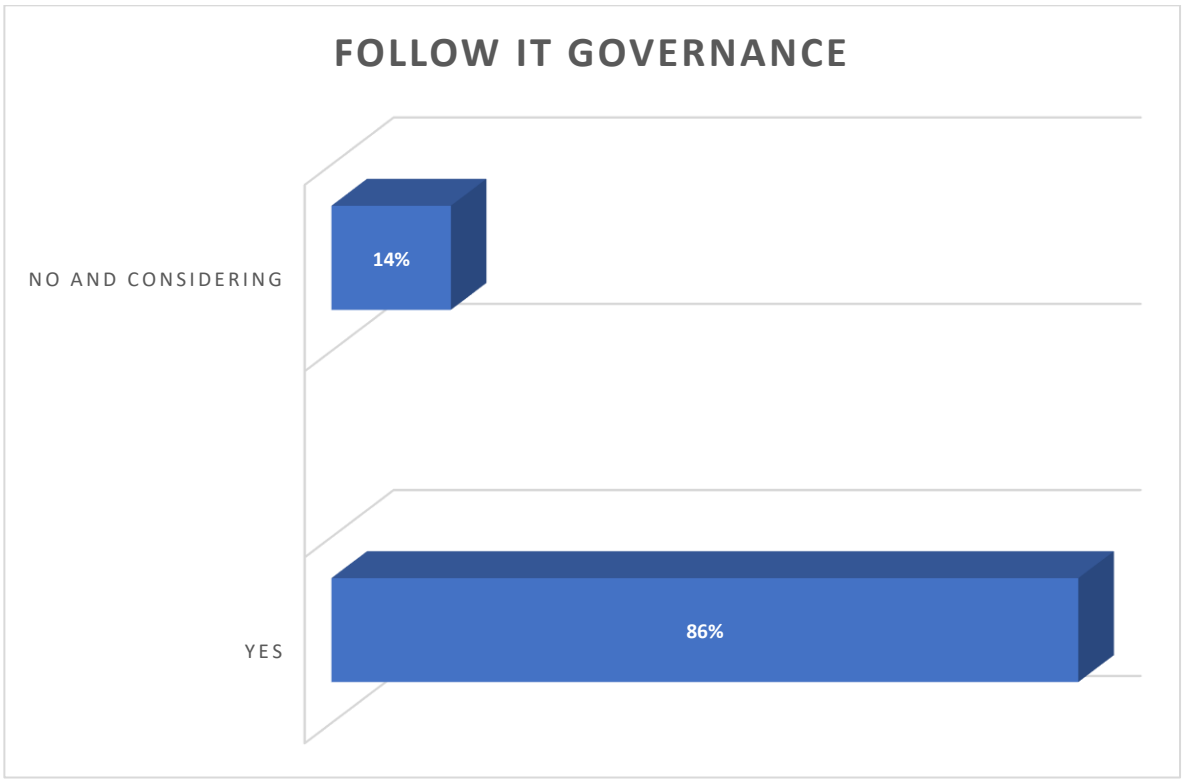

Figure 16 The Banks Adherence to Standard IT Governance Framework

Figure 16, shows that the majority of 86% of respondents indicated that the Banks are adherence to using standard ICT governance frameworks such as COBIT, ITIL, and ISO. However, 14% of the respondent indicated that the commercial banks that have not adopted ICT governance are considering the implementation of ICT governance standards.

4.1.9 Best Facts that Characterizes ICT governance at the Bank

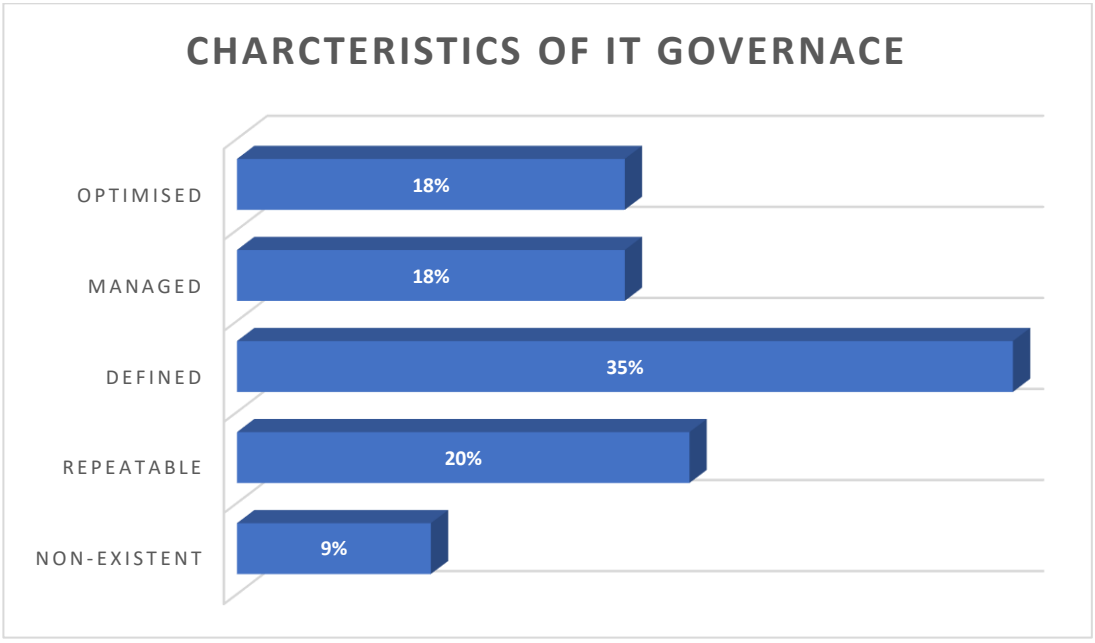

Figure 17 Characterizes ICT governance in the bank

From figure 17, shows that 35% respondents indicated that the commercial banks have the process defined where procedures have been standardized and documented, 20% of the respondent indicated that repeatable process is used where processes have been developed to the stage where similar procedures are followed by different people undertaking the same task. 18% of respondent indicated that Managed process is used and it is possible to monitor and measure compliance with procedures and to take action where processes appear not to be working effectively. 18% of respondents indicated that the optimized process is used and processes have been refined to a level of best practice, based on the results of continuous improvement and maturity modelling with other organizations. 9% of the respondent revealed that no process level is been used to effectively IT resources.

4.1.10 Measure of the Effectiveness of ICT governance Strategies

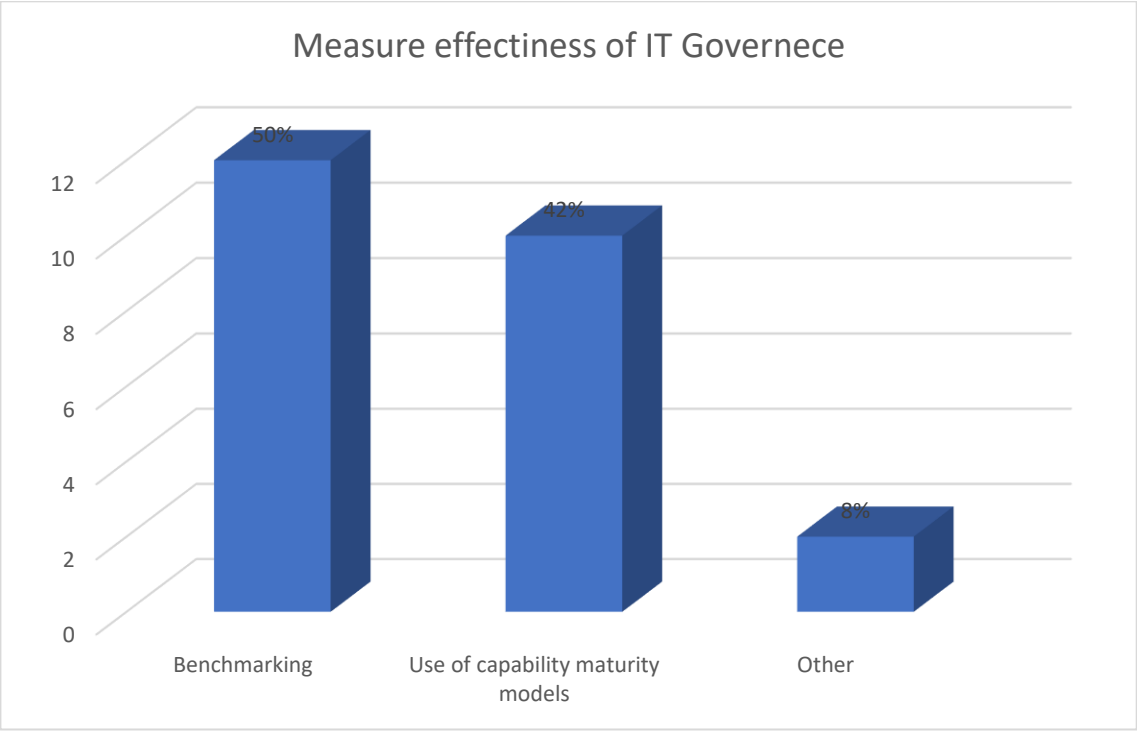

Figure 18 Measure of Effectiveness of ICT governance Strategies

From figure 18, half of 50% of the respondent indicated that they measure the effectiveness of the ICT governance within the organizations through benchmarking. 42% of the respondent indicated that they measure the effectiveness of ICT governance through the use of capability maturity models like capability maturity models. 8% revealed that they use other means of measuring the effectiveness of ICT governance.

4.2 ICT governance Levels

4.2.1 Participants disagreeing the existence of ICT governance

In order to investigate the elements of ICT governance in the commercial banks, the study used a Likert scale in which 5(100-80%),4(80-60%),3(60-40%),2(40-20%) and 1(20-0%) represented continuum scores for *Very Large Extent, Moderately large Extent, Moderately Low Extent, Very Low Extent, and No Extent respectively*. These enabled the tabulation and interpretation of the responses from the research instrument. The main statistics derived are mean, standard deviation and variance. The mean illustrated the extent to which the respondents agreed or disagreed with the statements put forth on the Best practices of commercial banks based on ICT governance in Zambia as shown on figure 19.

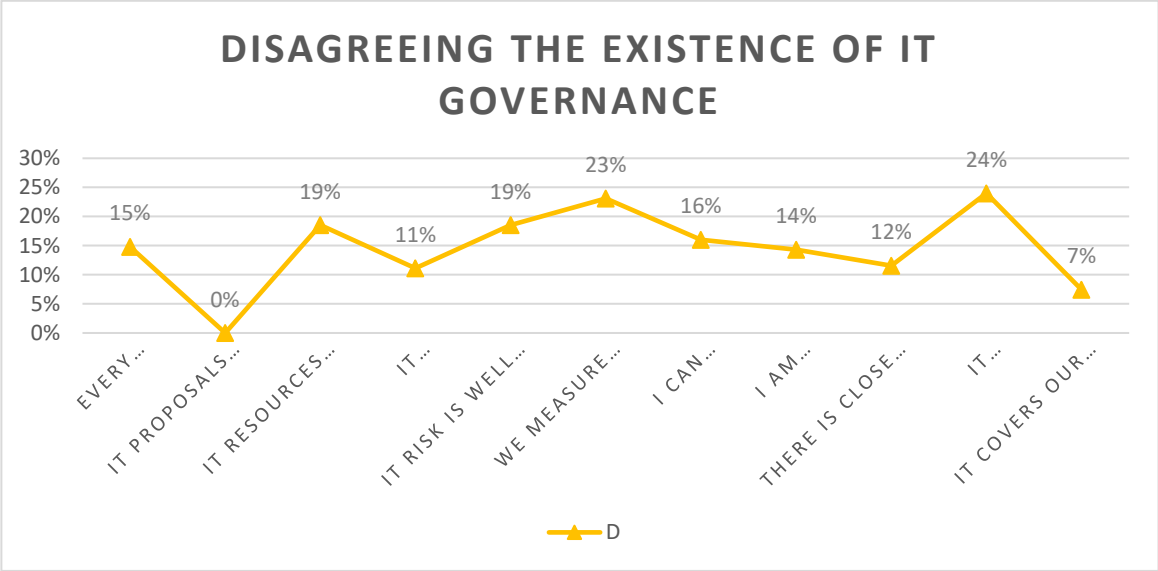

Figure 19 Disagreeing the existence of ICT governance

Figure 19. Shows how the respondent disagreed with elements on ICT governance in the commercial banks. 24% of the respondent with the rating of very low revealed that ICT governance is not separate from IT in the commercial banks. 19% of the respondent also thought that risk is not well managed and return on investment is not measured in the commercial banks. 15% of the respondent thought that employees were not conversant with ICT governance and that the proposals were not in line with IT strategy.

4.2.2 Participants agreeing with the existence of ICT governance

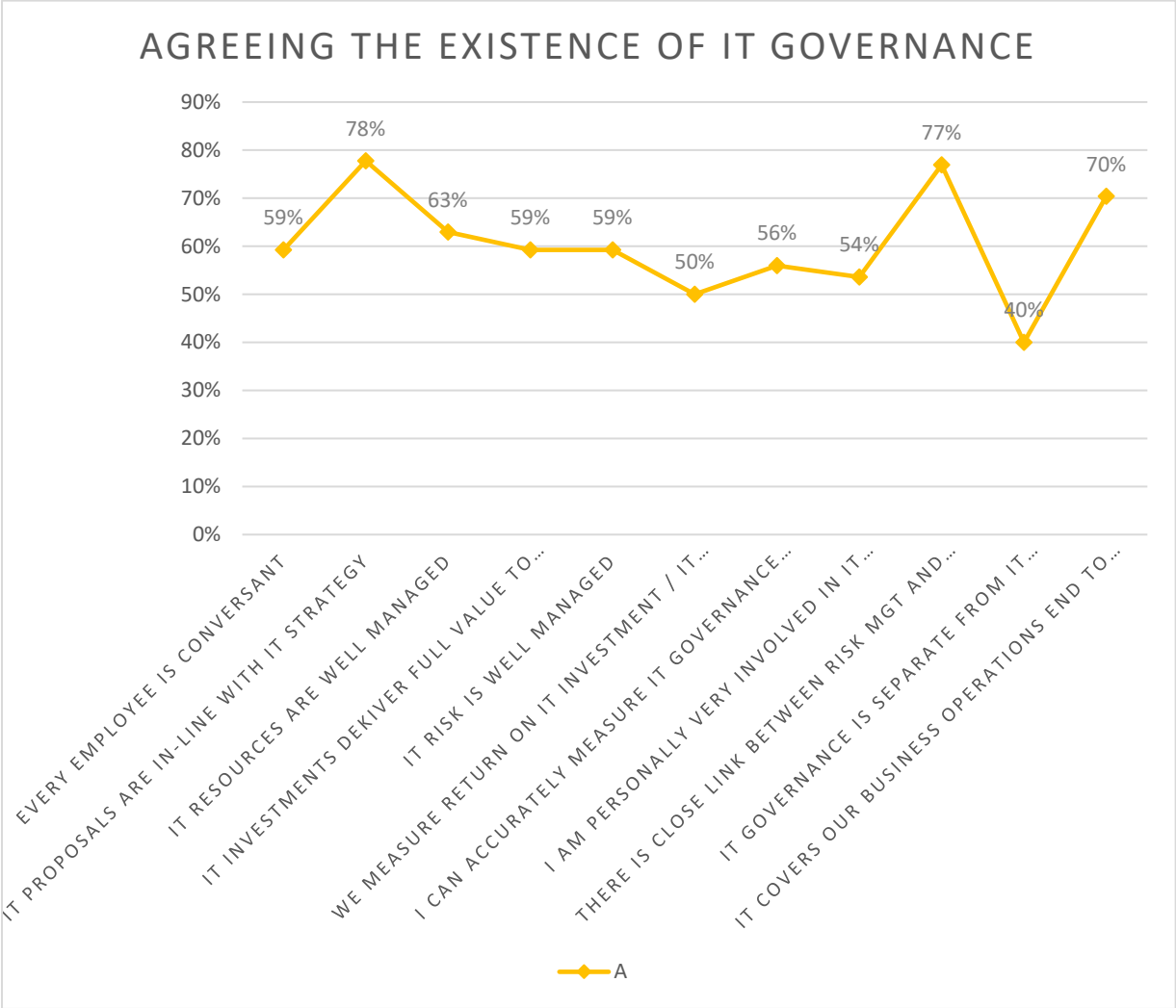

Figure 20 Agreeing the existence of ICT governance

Figure 20 shows 78% of the respondents overwhelming agreeing that the organization has its IT proposals in line with the approved IT strategy. 77% of the respondent thought there was a close link between risk management and business. 70% of respondents felt that IT covers the banks business operations from end to end hence the implementation of ICT governance has improved business operations.

4.2.3 Comparison of agreeing and disagreeing

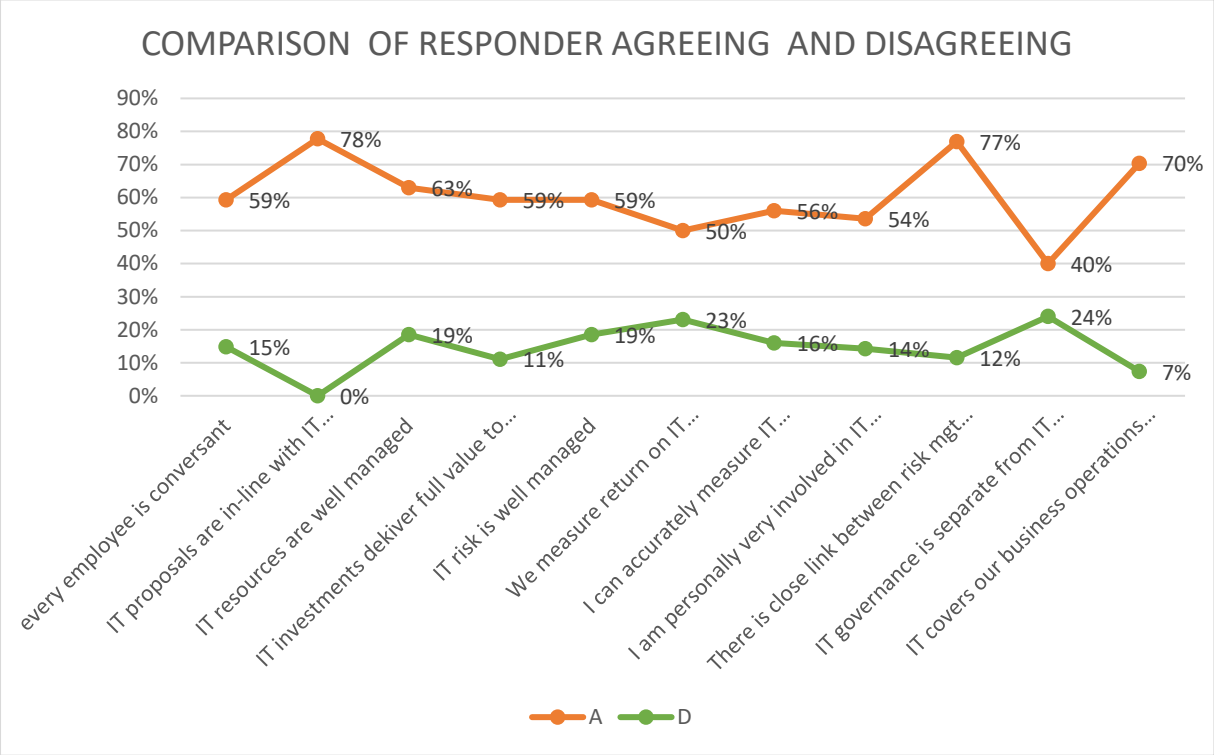

Figure 21 Disagreeing the existence of ICT governance

Figure 21 shows the comparison of the responses for those that agreed and those that disagreed with regards to the implementation of ICT governance. Those that agreed had the mean of 60% and those that did not agree had the mean of 21% responses. Looking at the graphs in regards to the levels of ICT governance in the commercial banks the study revealed the majority 70% of the respondent thought IT covers business end to end and the minority of 7% disagreed, this represented the mean of 39% and the standard deviation of 45% of the responses. The study also revealed the majority 59 % felt that risk was minimized in the commercial bank through the implementation of ICT governance, a mean of 39% and a standard deviation of 28%. The study also revealed that the majority of 78% thought that through the implementation of ICT governance the IT Proposals in the commercial banks were in line with IT strategy while no responder disagreed; this showed the mean of 39% and a standard deviation of 55% respectively

4.2.4 Assessment Levels of ICT governance

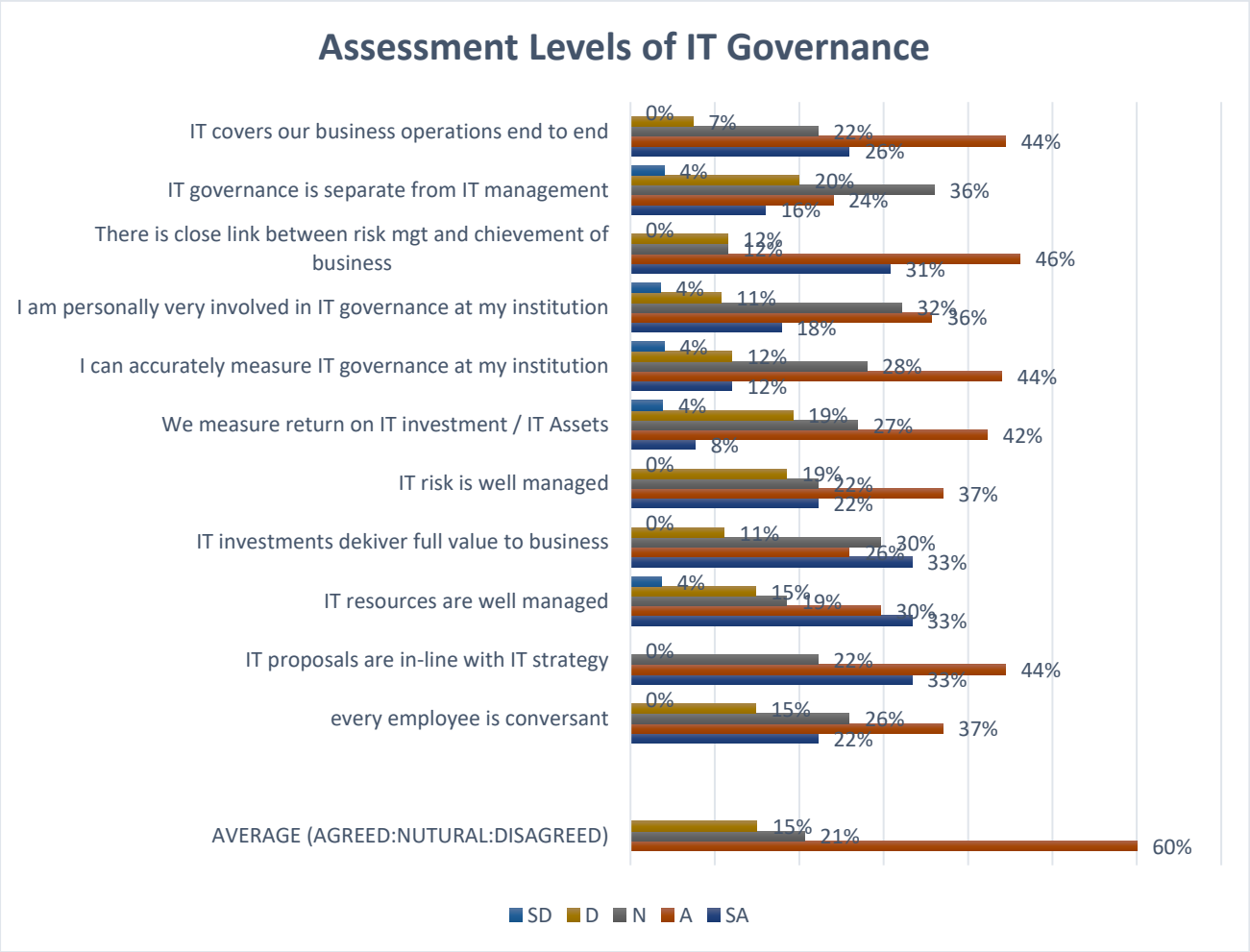

Figure 22 Assessment Levels of ICT governance

As depicted in figure 22 above. On average for the assessment, 60% of the respondent agreed that there some levels of governance been practised in the commercial banks. The study revealed that 21% of the respondent opted to remain natural for the reasons known to themselves and 15% of the respondent disagreed that there are some levels of ICT governance in the commercial banks. The research also found that respondents were able to accurately describe ICT governance at their institution with a mean representation of 60%.

4.3 Challenges of ICT governance framework Implementation

In order to investigate the elements of ICT governance in the commercial banks, the study used a Likert scale in which 5(100-80%),4(80-60%),3(60-40%),2(40-20%) and 1(20-0%) represented continuum scores for *Very Large Extent, Moderately large Extent, Moderately Low Extent, Very Low Extent, and No Extent respectively*. These enabled the tabulation and interpretation of the responses from the research instrument. The main statistics derived are a mean and standard deviation. The mean illustrated the extent to which the respondents agreed or disagreed with the statements put forth on the challenges hindering the successful adoption of an ICT governance framework in Zambian commercial banks. This is well elaborated in Figure 20 and narratives which show the respondents and the statistics

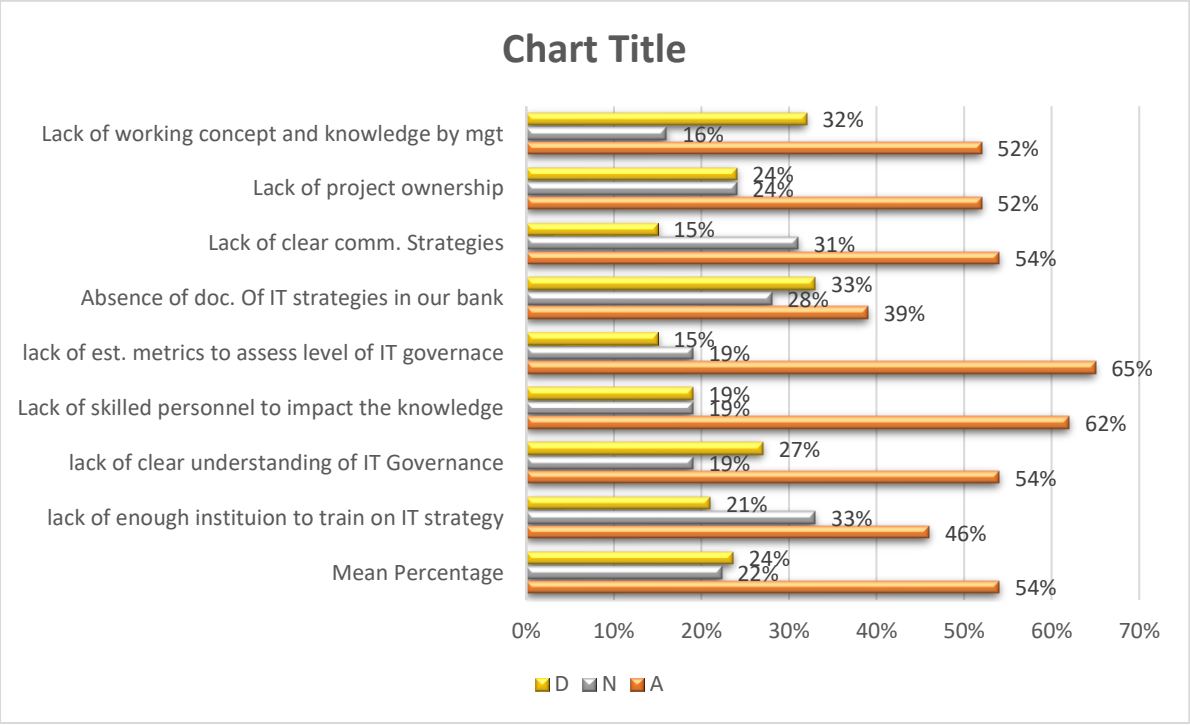

Figure 23 Challenges of ICT governance framework Implementation

As depicted from the figure above. Assessment of the responses about the hindrances of ICT governance adoption, 54% of the respondent agreed, 24% disagreed and 22% opted to remain neutral. The study also revealed a standard deviation of 8% for those that agreed, 6% for those that did not agree and another 6% for those that remained neutral.

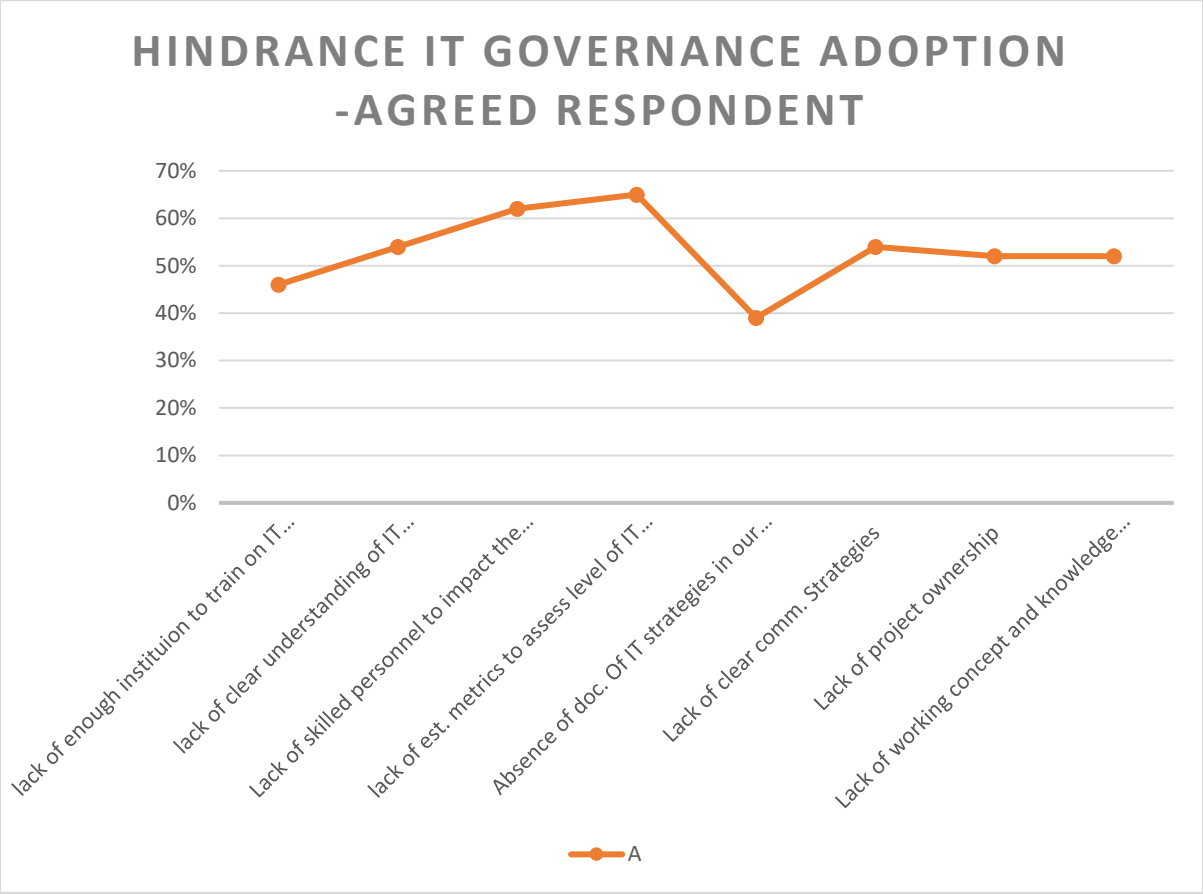

Figure 24 Challenges ICT governance Framework Adoption agreed

The study revealed that the majority of respondents felt that a lack of estimating metrics to assess the level of ICT governance was a major hindrance in implementing appropriate ICT governance framework. This represented 65% of the responders that agreed, 15% of the responders that did not agree and 19% of the responders that opted to remain neutral. The study also revealed a standard deviation of 28%.

62% of the respondent agreed that a lack of skilled personnel affected the successful adoption of ICT governance, 19% of the respondent disagreed that the lack of skilled personnel affected the successful adoption of ICT governance. This represented the mean of the response of 33% and the standard deviation of 24%

Another hindrance that the study uncovered was a lack of a clear understanding of ICT governance across the banks. 54%, a rating of moderately low extent was recorded for those that agreed, 19% for those that did not agree and 27% opted to neutral. This recorded a mean response of 30% and a standard deviation of 18%.

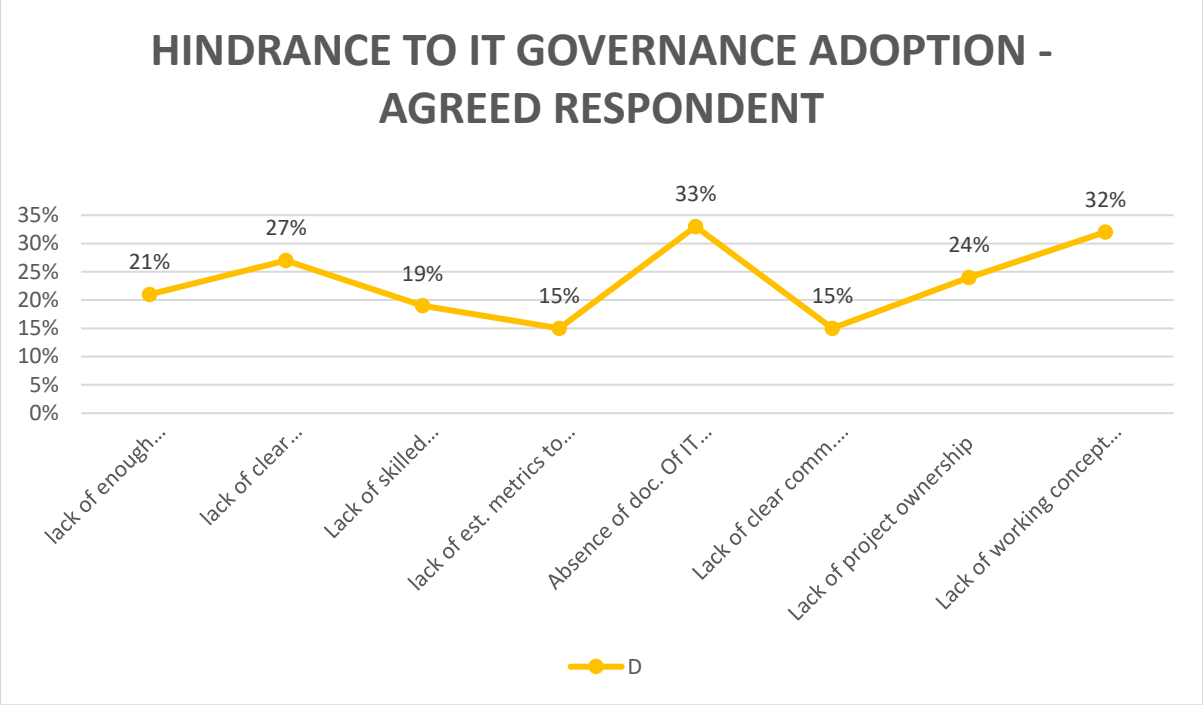

Figure 25 Challenges ICT governance Framework Adoption Disagreed

Table 7. shows a graph for the respondent that disagreed. 33% respondent strongly disagreed that absence of IT strategies is the hindrance to the successful adoption of ICT governance and it was followed by 32% that felt that lack of working concept and Management knowledge was a hindrance to ICT governance adoption.

4.5 ICT governance study findings

Studies have shown that IT Governance practices once adopted and implemented may facilitate the IT-business strategic alignment and creates value for organisation stakeholders. However, this section has captured the global COBIT enterprise governance structure (4.5.1) and compared with the research finding on governance structure in the Zambian bank (4.5.2). Finally, the study proposes a bank organisation governance structure model (4.5.5).

4.5.1 Global enterprise governance structure

ICT governance has been implemented by several organizations globally with the view of aligning IT to business objectives. The implementation of ICT governance through COBIT 5 covers all functions and processes in an organization, not just the IT department function. The first phase begins with COBIT 5 process EDM01 that ensure governance framework setting and maintenance, which is responsible for defining the governance system used by the

organization. The process is composed of three governance practices that evaluate, direct and monitor the governance system. All the outputs of these practices are inputs to other processes of the EDM domain, i.e., EDM01 is a prerequisite for the deployment of other EDM processes. This justifies starting the implementation of the model with this process.

Table 3 Enterprise governance structure (ISACA, 2012)

EDM01 RACI Chart																										
Key Governance Practice	Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Business Executives	Business Process Owners	Strategy Executive Committee	Steering (Programmes/Projects) Committee	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information Security Officer	Architecture Board	Enterprise Risk Committee	Head Human Resources	Compliance	Audit	Chief Information Officer	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
EDM01.01 Evaluate the governance system.	A	R	C	C	R		R				C		C	C	C	C	C	R	C	C	C					
EDM01.02 Direct the governance system.	A	R	C	C	R	I	R	I	I	I	C	I	I	I	I	C	C	R	C	I	I	I	I	I	I	I
EDM01.03 Monitor the governance system.	A	R	C	C	R	I	R	I	I	I	C	I	I	I	I	C	C	R	C	I	I	I	I	I	I	I

4.5.2 Governance Structure for Zambian Bank

Table 4 Leadership Structures of banks in Zambia

	Governance Practice	Board	Chief Exective Officer	Chief Financial Officer	Chief/Director Information Officer	Chief Operations Officor	Chief Information Security Officer	Chief Risk Officer	Chief Retail Officer	Chief/Head Audit Officer	Chief/Head of Legal	Chief/Head of Compliance	Information Security Managers	Head of IT
	Structures of Banks													
1	Access Bank Zambia Limited	✓	✓	✓		✓		✓						
2	Atlas Mara Bank Zambia Limited	✓	✓	✓		✓		✓	✓	✓	✓			✓
3	Bank of China Zambia Limited	✓	✓	✓		✓		✓						
4	Barclays Bank of Zambia	✓	✓	✓		✓		✓		✓	✓	✓		✓
5	Cavmont Bank Limited	✓	✓	✓		✓		✓	✓					✓
6	Citibank Zambia Limited	✓	✓	✓		✓		✓	✓	✓	✓	✓		✓
7	Ecobank Zambia Limited	✓	✓	✓		✓		✓					✓	✓
8	First Alliance Bank Zambia Limited	✓	✓	✓		✓		✓						✓
9	First Capital Bank Zambia Limited	✓	✓	✓		✓		✓	✓	✓	✓			✓
10	First National Bank of Zambia Limited	✓	✓	✓		✓		✓						✓
11	Indo-Zambia Bank Limited	✓	✓	✓		✓		✓	✓					✓
12	Investrust Bank Zambia Limited	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓		
13	Stanbic Bank Zambia Limited	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓		
14	Standard Chartered Bank Zambia Plc.	✓	✓	✓		✓		✓	✓	✓	✓	✓		
15	United Bank for Africa Zambia Limited	✓	✓	✓		✓		✓	✓	✓	✓	✓	✓	
16	Zambia Industrial Commercial Bank Limited	✓	✓	✓		✓								✓
17	Zambia National Commercial Bank	✓	✓	✓		✓		✓	✓	✓	✓	✓	✓	✓
	Bank of Zambia	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	

Table 4 shows a table representing the structures in the Zambian banks. From the table above, shows that only 3 banks have IT department represented at the C level or reporting direct to Chief Information Officer / Managing Director in Zambia. The table also shows that Information Security is not represented at C Level and the IT department is reporting to the Chief/ Director Operations officer. The study revealed that all the banks have the Finance, Operation, and Risk represented at the C. level. IT was also noted that all the banks had a board of directors and committees in place.

4.5.3 Proposed bank organisation structure model

Below is a proposed bank governance structure model that includes IT and Security in the bank's corporate governance structure;

Step 1: BoZ ACT

Through the guide of **ECTA [A]**, Central Bank (BoZ) issues a directive or ACT to compel the banks to establish good corporate governance based on COBIT EDM01 process. The Board of Directors compels management to include the Information Technology and Information Security in the Executive Management structure of the banks.

Step 2: Governance

The proposed model bank governance aims at separating governance from management as per COBIT EDM01. Separating governance and management promotes accountability at all levels. In the context of the model, **governance** [B] is responsible for offering oversight and decision-making related to strategic direction, financial planning, and bylaws called the policies. **Policies [C]** are set of rules and laws that outline the organization's purpose, values, and structure. Governance provides a mechanism for good enterprise governance that focuses on stakeholder value by balancing performance and conformance. **Stakeholders** are the owners or shareholders and receive dividends when the organisation is making a profit. Shareholders appoint the **Board of Directors** to oversight and strategic direction to Management through policies.

Step 3: Management

Management [D] on the other hand, mainly involves controlling in alignment with the direction set by governance. The (executive) management team under the leadership of the **chief executive officer** or managing director is ultimately responsible for this. Again using the political system an illustration, it may imply the roles played by differing government parastatals, agencies and departments in Zambia. Management develops a **strategy [E]** from the polices so that they may run routine decisions and administrative work related to the daily operations of the **organization [F].**

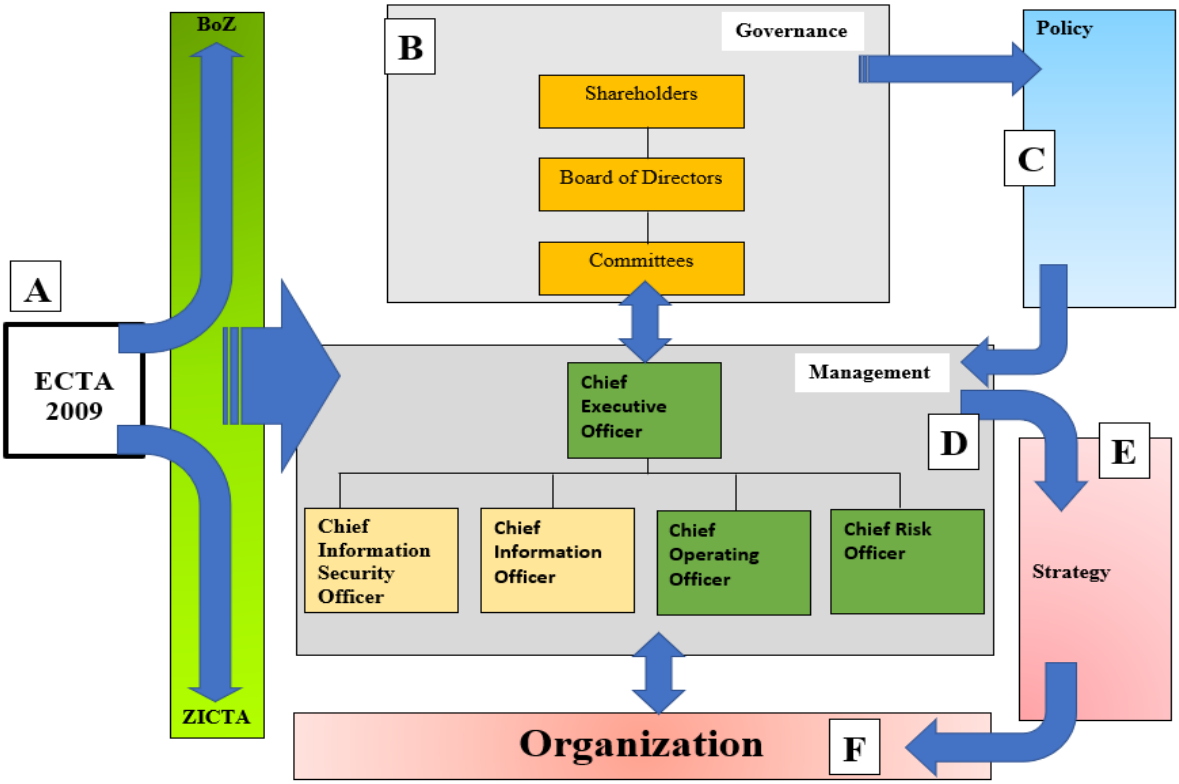

Figure 26 Proposed Bank Governance Structure Model

4.5.3 Proposed bank Information security governance model

Below is a proposed bank information security governance strategy model that includes all the layers of information security asset protections.

The rising tide of cybercrime and threats to critical information assets mandate that boards of directors and senior executives are fully engaged at the governance level to ensure the security and integrity of those resources. Below are components of the bank information security governance model cascaded from the bank governance stricture model

Layer 1: Physical

The physical layer in the model is very cardinal to the banks. Physical controls improves security for the banks. These controls are put in place to ensure that only authorized individuals can access certain areas or perform specific actions. The model proposes an optimized use of Access cards, closed-circuit television (CCTV) and Security officers at the physical layer.

However, the research found that some assets like ATMs were not secured and intruders could install schemers to steal funds from customer's accounts. The research also found the physical controls were not adequately implemented as bank visitors were not escorted within the banks by the security officers. Security governance and management around the physical controls should be improved in order to protect the banks from cyber attacks.

Layer 2: Network

Network security is very important for the banks. The bank's assets can easily be compromised if there no good security governance around the network are put in place since networks are entry points for every organisation.

However, the model proposes good security governance controls by using firewalls on the perimeter to stop intruders before enter the bank networks. The banks are to sets up VPN to encrypts data flowing through the network, and encrypts data at rest. Even if attackers get past the firewall and steal data, the data is encrypted.

Layer 3: Endpoints

Security information Event Managers (SIEM) and antivirus software is critical to protecting endpoints against unauthorized changes, viruses and malware.

Layer 4: Applications

Good security governance procedure guide like OWASP and SDL needs to be adopted when writing codes for organisation's **applications** to avoid data breach.

Layer 5: Data

Data or Information is the most valuable asset for all the organisation's and such appropriate data classification needs to be established to determine the level of security controls to be implemented.

Layer 6: Enterprise

An organisation is a network of people, assets and processes interacting with each other in a defined roles and working towards a common goal.

Layer 7: Business Objectives

Enterprise's strategy specifies business goals and objectives to be achieved as well as the values and missions to be pursued. It is a set of directions of the enterprise However, the IT security strategy should be able adapt to the changes in the external and internal factors.

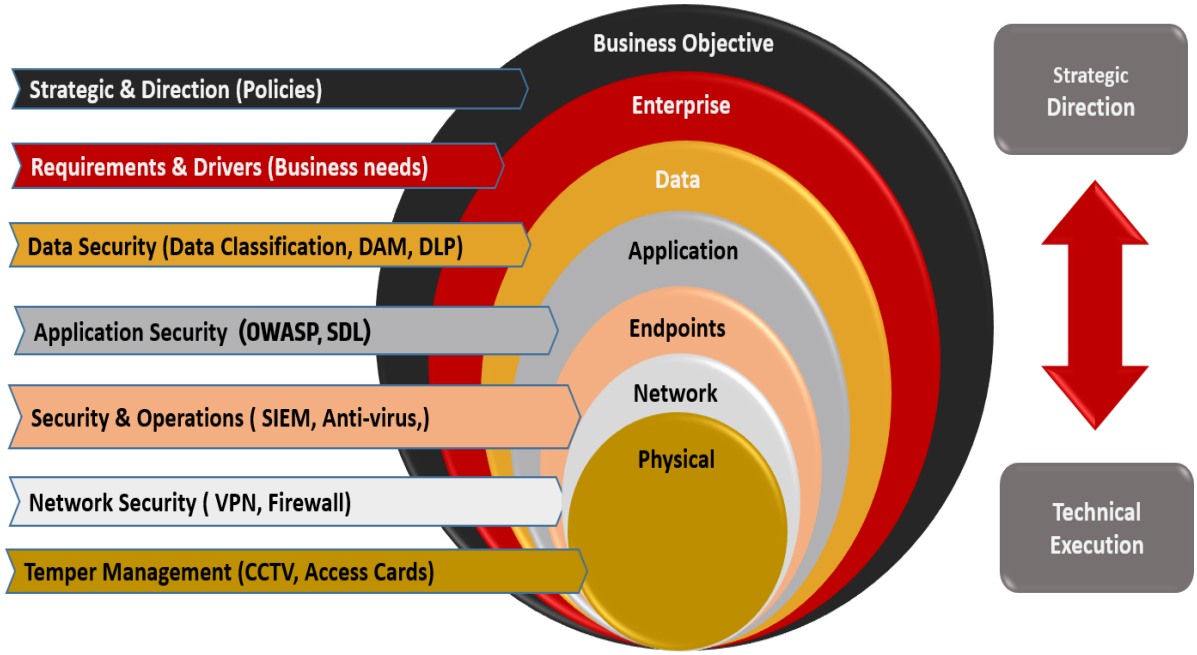

Figure 27 Bank information security governance model

Chapter 5

DISCUSSION AND CONCLUSIONS

5.1 Discussion

The study revealed that foreigners own the majority of the commercial banks. However, 47% of the respondent indicated that the foreigners owned their banks, 30% indicated that their banks had the ownership shared between the Zambians and foreigners and locals owned 23% of the respondent indicated were owned locally while a similar study in Kenya showed that, foreigners own 56% opposes to Zambia where foreigners own 47% (JOHN, 2015). The study revealed that most commercial banks are falling between 26-50 branches. This represented a response of 64% for between 26-50, between 11-25 accounted for 20%, above 50 accounted 10%, between 6-11 that accounted for 3% and 3% for between 1-5 branches while branches range between 1 and 16 (JOHN, 2015). In interviews, the commercial bank's IT representatives indicated that Optical fibre connected the branches to the main office. The study also revealed most of the banks use Client-Server Topology where a server is located at central management and branches computers connect to the main server the main systems are located at the head office (Lammle, 2016). This, therefore, means that customer information is located at the head office and should be transmitted in a secured manner.

The study also revealed that the majority of respondents had the titles not specifically asked in the questionnaire representing a 55%, 23% of the responders were Managers, 19% business unit executive or unit heads and least of the responders of 3% was Chief Information Officer while Kenya had the majority from the Chief Information Officers (JOHN, 2015). In Zambia, most of the Chief Information Officers delegated the role to complete the questionnaire to their managers and were only available for interviews. It also noted that the strategy committee meets quarterly (42%) and some monthly (39%) look at how they can implement and plan good strategy processes for ICT governance. The research also noted that the review of budgets and plans is done regularly to conform to the ICT governance implementation while in a similar study Kenya the board of directors regularly meets to discuss the budget and plans (C.L.Parmo, 2009). COBIT through the Evaluation, Delivery, and Monitory (EDM 02) process recommends the prudent use of IT resources so that value can be created for the shareholders which means that strategic meetings are very important for the organization's success. The monthly 39% and

quarterly (39%) meetings give a total of 81% indicating that the strategic committee meets and that means some good level of ICT governance is been practised in the banks. The COBIT 5 Evaluate, Direct and Monitor (EDM) process set is designed to govern and encapsulate the processes of all other management processes (Menevse, 2011).

There is a divide of the respondent in regards measure of the effectiveness of ICT governance strategies in the Zambian commercial banks as 50% indicated that they were using benchmarking and 42% using the Capability Maturity Model. Benchmarking is a tool used to measure performance by comparing with the competitors and identifying the gaps. Commercial banks used the Capability Maturity Model to assess the maturity of some processes by grouping them into different categories. The tool further helps commercial banks to benchmark its process against the process for other banks (Pasquini, 2013). This is in alignment with COBIT process Align, Plan and Organize (APO04) that talks about a measure for the effectiveness of ICT governance strategies. The total results of 92% respondent indicated that they measure ICT governance strategies through Benchmarking and Capability Maturity Model. This means COBIT process APO is working effectively in the banking sector.

There was a divide of the respondent about the characteristic of ICT governance. 35% indicated that the commercial banks were using a defined process where procedures have been standardized and documented, 20% of the respondent indicated that repeatable process is used where processes have been developed to the stage where different people undertaking the same task follow similar procedures (Michael Broudy, 2016). 18% of respondent indicated that Managed process is used and it is possible to monitor and measure compliance with procedures and to take action where processes appear not to be working effectively. 18% of respondents indicated that the optimized process is used and processes have been refined to a level of best practice, based on the results of continuous improvement and maturity modelling with other organizations (Max Shanahan, 2011). Looking at the divide of the respondent and that only 18% indicated that the process is optimized , it's clear that processes have not fully matured to the optimized final level of the Capability Maturity of COBIT Process Assessment Model (PAM) and put on ISO/IEC 15504 process rating scale of (Not Achieved 0 to 15%; Partially 15% to 50%; Largely Achieved 50% to 85% and Fully 85% to 100%). Therefore, the level of governance can be computed from ISO/IEC 15504 process rating scale by totalling 3 levels Defined (35%), Managed (18%)and Optimized (18%) and the total 71%. The computed 71%

total falls between 50% and 85% on ISO/IEC 15504 process rating scale meaning that ICT governance is largely achieved but not fully achieved as per COBIT process.

Based on the mean value of 60%, the majority respondent agreed that there some levels of ICT governance been practised in commercial banks. 78% of the respondents overwhelmingly agreed that the organization has its IT proposals in line with the approved IT strategy. 77% of the respondent thought there was a close link between risk management and business. 70% of respondents felt that IT covers the bank's business operations from end to end hence the implementation of ICT governance has improved business operations. However, the research found that respondents were able to accurately identifying ICT governance at their institution and there was a need to map the processes and identify the gaps (C.L.Parmo, 2009). Based on the responder's responses, the research indicated that banks customized processes in-line with COBIT 5 principle number 3 (apply a single integrated framework). COBIT 5 Principle number 3 encourages the organization to customize the COBIT processes into the organization's business requirement (Max Shanahan, 2011).

The central bank of Zambia has been at the forefront in ensuring commercial banks adopt ICT governance principles that address risks and enhances accountability and performance. Through the bank of Zambia directives, it was clear that the commercial banks were encouraged to adopt good IT and corporate governance and should have the position of Chief Risk Officer (Zambia, 2016). The research revealed that all the commercial banks complied and had the position of Chief Risk Officer and this is in alignment with the COBIT 5 EDM process (Joanne De Vito De Palma, 2016). The study further revealed that IT alignment is the highest-rated driver and desired outcome of ICT governance practices.

The study revealed that the majority of respondents felt that there is a lack of estimating metrics to assess the level of ICT governance in the banks and that was a major hindrance in implementing appropriate ICT governance framework (Paul A. Williams, 2015). This represented 65% of the responders that agreed, 62% of the respondent agreed that a lack of skilled personnel affected the successful adoption of ICT governance. Another hindrance that the study uncovered was a lack of clear understanding of ICT governance across the banks and 54%, of the respondent, agreed. The respondent thought that the ICT governance young is a field hence been misunderstood by the employees in the banks. However, there is a need to

train the entire organization's workforce on ICT governance best practices and the implementation of COBIT in the organizations.

Furthermore, many of the respondents felt that there is room for improvement for the implementation of ICT governance in both commercial banks and other organizations both public and private especially when it comes to automating the record-keeping and reporting of the various related operations. Many respondents thought that they would be more effective if they applied ICT governance not only to conform to regulations but also to achieve the desired business alignment, ensure value delivery, manage risk and provide a mechanism to measure IT performance as well as manage the resources well for better business operations and continuity (C.L.Parmo, 2009).

The research revealed that all the banks had operation structures where the Board of directors was overseeing the Governance of the banks and Executive Management was in charge of the management of the banks. This indicated that good governance has been practised in the banks as per COBIT principle number 5 (Separate Governance from Management) that recommends organizations to establish separation of Governance and Management in the organization. (Ndlovu, 2016). The operation structures of the banks showed that the Board of Director were reporting directly to the shareholders (the owners of the banks) and Management was reporting to the Board of Directors (Krishna Seeburn, 2014). The research also revealed that the Chief Executive Officer (CEO) of the banks was appointed by the Board of directors. The CEO appointed the executive management of the banks and this in alignment with COBIT 5 ICT governance EDM02 process best practice (Max Shanahan, 2011). The executive management headed the departments and the entire organizations reported to the Executive Directors. The bank's Management structure was alignment with COBIT 5 process APO09 management best practice (Bobbett R. Fagel, 2014).

Further, the study revealed weaknesses in the Executive Management for some of the banks did have Information Technology and Information Security as divisions headed by Executive Director. This is a major weakness in the bank structure COBIT APO09 process for key management practice that recommends Information Technology and Security should be a Division and represented by an Executive Director (Krishna Seeburn, 2014). The banks that do not have IT and security represented at C-level or Executive Directors run with the risk of IT requirements not properly represented to the Board of Directors and Board of Directors not

being able to know the Information Security risk the banks are running with (Micheal Broudy, 2016). The research also revealed that IT is no longer a back-office function but it is considered as part of business as a business enabler and as such, it should be placed at C-Level where it supposed to be not a department within a division whose Executive Director may not fully understand and articulate IT requirements at C-Level (CLARKE, 2014). The position of Chief Information Systems Officer (CIO) has become an important role due to the numerous business and technical responsibilities assigned to the organization's top executive management. ICT governance best practice recommends that CIOs should ensure the firms IS investments are continually aligned with its strategic business objectives, while also planning and maintaining an IT infrastructure that will meet the firm's current and future information processing needs (Sellitto, 2012). However, out of the 17 commercial banks and Central bank, the study revealed that only 3 banks have IT department reporting directly to Chief Executive Officer / Managing Director in Zambia (Sellitto, 2012). The study also indicated that none of the banks had the role of Chief Information Security offer on the structure and represented at C Level. The study also captured that IT department reports to Chief/ Director Operations officer and Information Security in some banks report to Director/ Head IT and in Some banks reports to the Chief Risk Officer. The study revealed that all the banks have the Finance, Operation, and Risk represented at the C. level. IT was also noted that all the banks had a board of directors and committees in place (Hunter, 2010).

5.2 Conclusions

The first bank was established in 1956 and was called the Bank of Rhodesia and Nyasaland. Before independence, 3 foreign commercial banks dominated the banking sector namely Standard Chartered Bank, Barclays Bank, and Grindlays Bank providing fringe competition After the Mulungushi reforms of 1968, the government embarked on establishing financial institutions rather than nationalizing the existing ones. In 1969, ZANACO a first national commercial bank was established. In the same year of 1969, the republican government also established Non-Bank Financial Institutions such as the Zambia National Building Society, the Zambia National Provident Fund (NPF) and the Zambia State Insurance Corporation (ZSIC).

The banks in Zambia know good ICT and Security governance practices. The results were computed in ISO/IEC 15504 process rating scale of (Not Achieved 0 to 15%; Partially 15% to 50 %; Largely Achieved 50% to 85% and Fully 85% to 100%). However, it was clear that ICT

governance had not fully matured, and was at 60%. The study also noted that the practices like Asset Management, Contract Management, and Service Level Agreement are properly managed as per ICT governance best practices. The study also noted that the Government of Zambia has identified the need for ICT governance and has instructed all the parastatal companies like ZRA, ZESCO, NAPSA, and Bank of Zambia to formalize the deployment implementation of COBIT framework.

ICT and Security governance implementation, however, faces challenges like not having adequate resources and buy-in from the stakeholders to embrace it. To address ICT governance challenges in banks; appropriate processes and procedures have been put in place to measure the performance of IT systems and its alignment to the business objectives. These processes and procedures are implemented through the utilization of COBIT 5. Through the implementation of ICT governance, banks will effectively align IT objectives to bank corporate governance.

The banks have operation structures and the Board of directors was overseeing the Governance of the banks, and Executive Management was in charge of the management of the banks. This indicated that good governance has been practised in the banks as per COBIT principle number 5 (Separate Governance from Management) that recommends organizations to establish separation of Governance and Management in the organization. The operation structures of the banks showed that the Board of Director were reporting directly to the shareholders (the owners of the banks) and Management was reporting to the Board of Directors. The research also revealed that the Chief Executive Officer (CEO) of the banks was appointed by the Board of directors. This meant that study objective number 1 and 2 was achieved since the study was to investigate operations of the banks and the ICT governance practices systems in place.

The study revealed weaknesses in Executive Management for some of the banks. It was noted that out of the 17 banks under study only 3 had representation IT in Executive Management of the Banks and none of the 17 banks had a representation of IT Security at Executive Management. Despite IT being the cornerstone of the banks and the threat cybersecurity has on the IT infrastructure, the banks did not have Information Technology as a division headed by Executive Director. The banks were not in alignment with the COBIT process APO09 since they did not have IT and Security in their corporate governance key management practice. This requirement is in-line with the study objectives 1 and 2 that aimed at determining the operation structures and the ICT governance practices in the banks.

The Banks in Zambia use Information Technology (IT) and its infrastructure to deliver products and services. Through the use of Information Technology, banks were able to come up with innovative products and services hence gaining a competitive advantage over other banks. However, the banks will be required to conduct a gap analysis to identify the levels of compliance with the identified ICT governance frameworks. The study chooses COBIT as an ICT governance because it's a widely accepted ICT governance framework in the world and the republican government has instructed parastatal companies to adopt the COBIT framework.

5.4 Recommendation

Effective ICT and Security governance process is the cornerstone for many organisation as evidenced by the study. This is strengthened by the responses in the research. The banks should conduct a gap analysis to identify the levels of compliance with the COBIT framework. COBIT is a widely accepted ICT governance framework in Zambia and worldwide. Implementation of COBIT is central to the realization of value, strategic alignment and management of ICT related risks. The banks should put in place systems to ensure that there is simplicity in how the IT governance and conformation is practised. The bank should analyse the impact and the benefits of having the positions of CIO and CISO on executive management. Further assessment should be done on banks enterprise organization's to ascertain the roles and responsibilities and how much performance improvements the banks would benefit from the inclusions of the two positions. The banks should ensure that the organization's leadership, staff, policies, processes, practices, and technologies provide ongoing oversight, management, performance measurement, and course correction of all Information Technology activities. This function includes ensuring compliance with all external and internal requirements and education on ICT governance implementation to all the bank employees.

5.5 Further Work

Through the research design of this study, every effort was made to address methodological reliability, construct validity, internal validity and external validity, as a means for ensuring findings and conclusions were valid and consistent. Beyond the pure execution of the research, however, a number of other limitations are identified and discussed.

Firstly, given the theory-building nature of our study, we accept that our findings may not be transferable beyond the financial sector and as such, recognize that our proposed theory could

be strengthened through further empirical testing across a wide variety of organizational industries and sizes. Testing across different ICT governance routines would also be valuable to further validate and our model, however at this stage, we believe that the choice of the routine was less influential on the findings than the choice of industry type. It should also be noted that our proposed model may not be unique to ICT governance and may hold true for a more broad view of governance.

Secondly, despite the application of ICT governance practices the banks, it was discovered that ICT governance practices were not understood by all the bank employees as such the research scope sample was only targeted at the employees working in Information Technology departments for various banks. The other limitation was due to the sensitivity of the financial sector industry, some banks were unwilling to avail information to the researcher. Some of the employees feared that if it was known that they shared information they could lose employment. It was noted that the banks were afraid of losing face and confidence from the customers if it was discovered their banks were not properly managed.

For future research, we propose that our model be tested beyond the financial sector environment. By assessing the appropriateness of the model across a wide range of industry types would strengthen its external validity and add to its usefulness as theory. Hypotheses based on the constructs identified within our study could be established and validated through a cross-sectional survey.

REFERENCES

1Karim Youssfi, J. B. S. E., 2014. A Tool Design of Cobit Roadmap Implementation. *(IJACSA) International Journal of Advanced Computer Science and Applications,,* 5(7), p. 9.

4, S. N., 1997. *THE CO-OPERATIVE SOCIETIES ACT.* s.l.:Act SI.

Act, B., 2017. Co-operative Societies of the State and the finance and backing. p. 92.

Adeoti, O. O., 2013. Challenges to the efficient use of point of sale (POS) terminals in Nigeria. *African Journal of Business Management,* 7(pp. 2801-2806,), p. 6.

Agboola, A., 2007. *Information and Communication Technology (ICT) in Banking Operations in,* s.l.: Obafemi Awolowo University.

Ahsan, M. S. K., 2016. ROLE OF ENTERPRISE ARCHITECTURE IN HEALTHCARE ORGANIZATIONS AND KNOWLEDGE-BASED MEDICAL DIAGNOSIS SYSTEM. *JISTEM - Journal of Information Systems and Technology Management,* 12(2), p. 12.

Alawode, A. J. a. E. U. K., 2011. INFORMATION AND COMMUNICATION TECHNOLOGY. *International Technology, Education and Environment Conference,* p. 5.

Alshammari, R. A. H. A. A. B., 2010. Analytical Study on Internet Banking System. *Jounal of Computing,* 2(6).

Anton, G., 2014. *THE IMPACT OF INTERNET BANKING ON THE USE OF.* s.l.:Kyiv School of Economics.

BAZ, 2017. *The Banking and Financial Act.* s.l.:BAZ.

Bobbett R. Fagel, S. M. F., 2014. *CISM Review 2014.* 14 ed. s.l.:ISACA.

BoZ, 2004. *Annual Report Bank of Zamabia,* Lusaka: s.n.

BOZ, 2016. *Directive.* s.l.:Bank of Zamabia.

Brownbridge, M., 2000. *FINANCIAL POLICIES AND THE BANKING SYSTEM IN ZAMBIA.* s.l.:s.n.

By Niina Mallat, M. R. a. V. K. T., 2004. Mobile Banking Services. *COMMUNICATIONS OF THE ACM,* Volume 47, p. 5.

C.L.Parmo, 2009. Enterprise Architecture, IT strategy and ICT governance. Volume 5, p. 151.

Chiumya, D. C., 2010. *The Regulation of Banks.* s.l.:Washington, D. C., CGAP..

CLARKE, J., 2014. *IT Strategic Planning.* From Australian Board and management Terms: ISACA.

Debra Mallette, C. C. C., 2011. Implementing COBIT® in your Organization. *San Francisco Chapter, Isaca,* Volume 12, p. 26.

Dr.G.Tulasi Rao, T. R., 2015. Role of Information Technology in Indian Banking Sector. Volume 17, p. 5.

Esselaar, O. H. a. P., 2003. *Country Survey,* s.l.: s.n.

Ettish, A. A., 2017. INTEGRATING INTERNAL CONTROL FRAMEWORKS FOR EFFECTIVE CORPORATE INFORMATION TECHNOLOGY GOVERNANCE. *Journal of Information Systems and Technology Management – Jistem USP,* 14(3), p. 10.

FIRDOUS, S., 2017. IMPACT OF INTERNET BANKING SERVICE QUALITY ON CUSTOMER SATISFACTION. *Journal of Internet Banking and Commerce,* Volume 22, p. 17.

George Mangalaraj, A. S., 2014. ICT governance Frameworks and COBIT. *Mangalaraj et al.,* p. 10.

Heffernam, S., 2005. *Morden Banking.* s.l.:John Wiley & Sons Ltd.

Institute, I. G., 2005. IT Alignment-Who-is-in-Charge. *ICT GOVERNANCE DOMAIN PRACTICES AND COMPETENCIES,* p. 30.

IONESCU, I. G., 2012. *CATEGORIES AND TYPES OF BANKING INSTITUTIONS.* s.l.:Annals of the University of Petroşani, Economics.

Jeff Tyree and Art Akerman, 2005. Architecture Decisions:Demystifying Architecture. *Postmodern Software Design,* p. 9.

Joanne De Vito De Palma, P. T., 2016. A Primer for Imlementing Governace of Enterprise IT. p. 52.

John Dooney, M. S.-S., 2016. How Centralized and Decentralized HR Department Structures. *the Society for Human Resource Management* , p. 10.

Kalima, 2001. Financial markets and economic growth in Zambia. *Master of Arts Dissertation, University of Botswana, Gaborone, Botswana,* p. 70.

KOSKOSAS, I., 2011. THE PROS AND CONS OF INTERNET BANKING: A SHORT REVIEW. *Business Excellence and Management, University of Western Macedonia, Kozani, Greece,* Volume 1, p. 10.

Krishna Seeburn, P. L. F. C. S. C. C. C. C. P., 2014. *Basic Foundational Concepts.* Student Book: ed. Mauricius: s.n.

Krishna, S. P., 2018. *ROLE OF CO-OPERATIVE BANKS IN FINANCIAL INCLUSION.* s.l.:SVPM's College of Commerce.

Krugel, G. T., 2007. Mobile Banking Technology Options. p. 57.

Lammle, T., 2016. *CCNA.* s.l.:Cisco Press.

Le Thanh Trung, J. W. L., 2013. Implementation. *COBIT® 5 Implementation,* p. 78.

M. Buckle, E. B., 2011. *Principles of banking and fi nance.* s.l.:University of London International Programmes.

Maguire, S. S. &. S., 2017. Enterprise Architecture by Sparx Systems & Stephen Maguire. p. 6.

Maimbo, S., 2002. New Evidence from Emerging Markets. *Journal of International,* p. 35.

Martínez, J. d. L., 2006. Access to Financial Services in Zambia. *World Bank Policy Research Working Paper,* p. 36.

Matthew K. Luka, I. A. F., 2012. *The Impacts of ICTs on Banks,* s.l.: International Journal of Advanced Computer Science and Applications.

Mian, A., 2003. Foreign, Private Domestic, And Government Banks:. *New Evidence from Emerging Markets,* p. 46.

Micheal Broudy, M. D., 2016. *CISM Review Manual.* 15 ed. s.l.:ISACA.

Mishkin, F. S., 2009. *THE ECONOMICSOF MONEY,BANKING,AND FINANCIAL MARKETS.* s.l.:Peason.

MOHAMMED ALAA H. ALTEMIMI, M. S. Z., 2015. ICT governance Landscape: Toward Understanding the Effective ICT governance. *Scholedge International Journal of Business Policy & Governance,* 12(11), p. 13.

Mohanty, L. C. a. R. P., 2007. *Understanding Value Creation: The Shareholder.* s.l.:s.n.

Muhammad, M. S. S. I. a. M. A., 2013. *Information and Communication Technology and Bank Performance in Nigeria,* s.l.: Federal University Dutsinma.

N.C.Centre, 2005. A Best Pratice guide for Decision-makers in IT. *Internation Jounal* , p. 22.

Ndlovu, S. L., 2016. Challenges of CoBIT 5 ICT governance Framework Migration. *International Conference on Information Resources,* p. 17.

Niaz, Y. A. a. A., 2010. *The delicate balance of internet banking and bricks and mortar offices,* s.l.: Gotland University.

Okon, N., 2017. HOW TO APPLY COBIT 5 IN GOVERNMENT: THE CBN STORY. p. 25.

Onifade, O., 2018. Seven COBIT 5 Implementation Pitfalls to Avoid. *D,* p. 2.

Orandi Mina Falsarella, C. A. S. C. J., 2017. Corporate Strategic Planning and Information & Communication Technology Planning: a project based approach. Volume 24, p. 12.

Osotimehin, O. A. K., 2012. Adoption of Point of Sale Terminals in Nigeria: Assessment of Consumers' Level of Satisfaction. *Research Journal of Finance and Accounting,* 3(1), p. 6.

Pankaj Kumar Singh, J., 2014. *Linking of Customer Satisfaction with Shareholders' value.* s.l.:Global Journal of Finance and Management.

Pasquini, A., 2013. COBIT 5 and the Process Capability Model. Improvements Provided for ICT governance Process. *Obuda University Keleti Faculty of Business and Management,* p. 10.

Paul A. Williams, F. C. P. W. C. U., 2015. *ICT GOVERNANCE DOMAIN PRACTICES AND COMPETENCIES.* s.l.:ICT governance Institute.

Payment, 2007. *National Payment System Act,* s.l.: Bank of Zamabia.

Prizzon, L. E. a. A., 2018. *A guide to multilateral development.* s.l.:odi.org.

Prizzon, L. E. a. A., 2018. *A guide to multilateral development banks.* s.l.:odi.org.

PwC, 2018. *Global Economic Crime and Fraud Survey,* Lusaka: Pwc Zambia.

Ramesh Radhakrishnan, 2004. IT Infrastructure Architecture Building Blocks. *Sun Professional Services,* p. 27.

Reixach, A. A. i., 2001. *The Effects of Information and Communication Technologies on the Banking Sector and the Payments System,* s.l.: Universitat of Girona.

Report, A., 2015. *REPORT OF THE AUDITOR GENERAL ON THE ACCOUNTS OF PARASTATAL,* Lusaka: Auditor General.

Robertson, B., 2002. Modeling Architecture and Infrastructure Planning:Domains to Patterns and Beyond. *Enterprise Planning & Architecture Strategies,* p. 23.

S M Kundishora, 2008. *The Role of Information and Communication Technology ICT) in Enhancing Local Economic Development,* s.l.: South West Zimbabwe.

Saadan, S. S. M. K. a. K., 2013. The Formal Design Model of an Automatic Teller Machine (ATM). *Lecture Notes on Information Theory,* Volume 1, p. 4.

Sabine Buckl, F. M. S. R. C. S. C. M. S., 2010. *A Conceptual Framework for Enterprise Architecture Design.* s.l.:s.n.

Santha Vaithilingam, M. N. a. M. S. m., 2006. *KEY DRIVERS FOR SOUNDNESS OF THE BANKING.* Volume 2 ed. s.l.:Journal of Global Business and Technology.

Shirley J. Ho, S. K. M., 2006. *The Impact of Information Technology on the Banking Industry,* s.l.: Queen Mary, University of London, UK.

Sikazwe, C., 2014. *THE CORPORATE GOVERNANCE LAW APPLICABLE.* s.l.:Univesity of Capetown.

Simonsson, M., 2008. *PREDICTING ICT GOVERNANCE PERFORMANCE: A METHOD FOR MODEL-BASED DECISION MAKING.* s.l.:Universitetsservice US-AB.

Sona Karkoskova, G. F., 2016. Extending MBI Model using ITIL and COBIT Processes. 6(4), p. 16.

Stella E. Igun, 2014. Strategic Impact of ICT on Modern Day Banking Nigeria. *International Journal of Strategic Information Technology and Applications,,* Volume 5(4), 78-93,, p. 4.

Taylor, T., 2016. *Principles of Economics.* s.l.:Macalester College.

TOGAF, 2012. Banking Industry Architecture Network & The Open Group. Volume 2, p. 20.

Vyas, V. J. A. G. A. A. Y., 2016. Dubai Customs COBIT 5 Implementation. p. 6.

WESUTSA, J. M., 2010. *THE IMPACT OF ICT ADOPTION ON FINANCIAL PERFORMANCE OF,* s.l.: UNIVERSITY OF NAIROBI.

Yadhu Ravinath, S. K. B., 2013. Backup Virtual Private Networks in Banks. *International Journal of Emerging Trends & Technology in Computer Scienc,* Volume 2.

Zambia, B. o., 2015. *NATIONAL PAYMENT SYSTEMS IN ZAMBIA,* Lusaka: Bank of Zambia.

Zanaco, 2017. *Annual Report.* s.l.:Zanaco.

ZECH, 2014. *Zambia Electronic Clearing House Rules,* s.l.: s.n.

LIST OF APPENDICES

Publication Certificates

ISSN 2320-9186

PUBLICATION CERTIFICATE

Global Scientific Journals (GSJ PUBLISHER)

THIS IS TO CERTIFY THAT OUR REVIEW BOARD HAS ACCEPTED RESEARCH PAPER OF

lemmy Mwanza

Levels of ICT Governance in the Zambian banks

Published In Volume 8, Issue 1, January 2020 Edition

January 13, 2020

Visit us at:
www.globalscientificjournal.com

COORDINATOR

EDITORIAL MEMBER

PUBLICATION · CHAIR

ISSN 2320-9186

PUBLICATION CERTIFICATE

Global Scientific Journals (GSJ PUBLISHER)

January 13, 2020

Visit us at:
www.globalscientificjournal.com

THIS IS TO CERTIFY THAT OUR REVIEW BOARD HAS ACCEPTED RESEARCH PAPER OF

Eliya Banda

Levels of ICT Governance in the Zambian banks

Published In Volume 8, Issue 1, January 2020 Edition

COORDINATOR | EDITORIAL MEMBER | PUBLICATION · CHAIR

Published Paper

GSJ: Volume 8, Issue 1, January 2020
ISSN 2320-9186

GSJ: Volume 8, Issue 1, January 2020, Online: ISSN 2320-9186

www.globalscientificjournal.com

Levels of ICT Governance in the Zambian banks

Lemmy Patrick Mwanza[1]
School of Engineering
Dept. of Electrical & Electronics Engineering
The University of Zambia
Lusaka, Zambia
[1]*e-mail: lemwanzo@gmail.com*

Dani Eliya Banda[2]
School of Engineering
Dept. of Electrical & Electronics Engineering
The University of Zambia
Lusaka, Zambia
[2]*e-mail: dani.banda@unza.zm*

This research seeks to broaden and strengthen the holistic understanding of ICT and Security governance effectiveness by specifically examining how ICT and Security governance practices provide a structure for banks to ensure that IT investments support business objectives. ICT and Security governance is one of these concepts that suddenly emerged and became an important issue in the information technology area. To address this objective, we investigate the operations of the banks, analyze IT governance practices and design an ICT and Security governance model and Information Security Strategy model that aligns Information Technology and Information Security with the corporate governance of the banks. Corporate Governance is the type of governance system that covers the organization's operations holistically. Corporate governances are cascaded to ICT and Security governance that covers and aligns IT strategy to the corporate business objectives. Therefore, Control Objectives for business-related technologies (COBIT) is one of the frameworks that is used for the implementation of ICT and Security governance in organizations. ICT and Security governance has been implemented by several organizations globally with the view of aligning IT to business requirements so that the shareholders may realize benefits from the investments. Locally, the Bank of Zambia has directed all the banks to implement good corporate governance. The republic of Zambia has also directed and mandated all the parastatal companies to formalize the implementation of the COBIT framework. In 2015, the auditor general indicated that all parastatal ICT audits were based on COBIT framework.

Keywords — ICT Governance, Strategy, Banks, model, framework

INTRODUCTION

Currently, Zambia has 17 registered banks and of these, 12 were locally incorporated subsidiaries of foreign banks, 2 were partially owned by the Government of the Republic of Zambia and 3 were locally owned (BoZ, 2017). Banks in Zambia use Information Communication Technology as the driver for product innovation and delivering services to the customers through branch network interconnections (Santha Vaithilingam, 2006). Through the use of Information Technology, banks are able to come up with innovative products and services hence gaining a competitive advantage over other banks. The rapid advancement of technology and the increase of use of ICT has introduced threats like mismanagement of resources, misalignment of IT to needs with business objectives and Poor performance. As a way to address challenges in the banks, appropriate processes and procedures needs to be put in place to measure the performance of IT systems and its alignment to the business objectives. Information Technology (IT) has to be aligned with the business strategy and objectives. One way to align IT services to business strategy is through ICT Governance. ICT Governance is set rules that run the organization through policies, standards and procedures that effectively manage external legal, regulatory and contractual compliance requirements relating to bank's use of information and technology (ISACA, 2012). A policy is a deliberate system of principles to guide decisions and achieve rational outcomes. However, policies are implemented as a procedure or protocol. Policies are generally adopted by the Board of or senior

governance body within an organization. Procedures are step by step sequence of activities on how to execute the policies. Procedures are developed and adopted by management (Hare, 2001). A standard is a repeatable, harmonized, agreed and documented the way of executing activities. Standards contain technical specifications or other precise criteria designed to be used consistently as rules. Many standards and frameworks have been developed to evaluate the maturity of the ICT governance in the organisations. Control Objectives for business-related technologies (COBIT) is one of the frameworks that is used for the implementation of ICT governance.

LITERATURE REVIEW

A. The use of ICT in the banking Sector

Rapid advancement in ICT has had a profound impact on the banking sector and the wider financial sector over the last two decades and ICT has now become a tool that facilitates banks" organizational structures, business strategies, customer services, and other related functions (Dr.G.Tulasi Rao, 2015). Effective use of ICT is assisting banks to be more customers centric in their operations by building a more solid foundation in the customer relationship management system. ICT supports banks grow a range of products/services while mitigating fraud levels and improving risk management, broaden the customer base, reduce transaction and operational cost and also help gain a competitive advantage over competing banks (WESUTSA, 2010). The application of IT within banks is manifested through Networked branches, Automated teller machines, Point of Sale Banking, Mobile Banking, and Payment Transfers e.g. RTGS and SWIFT.

All the banks in Zambia are integrated into the Payment Settlement System. BoZ Central Securities Depository System Rules Jan-20160 observes that Real-time gross settlement systems are specialist funds transfer systems where the transfer of money or securities takes place from one bank to another on "real-time" and a "gross" basis (S M Kundishora, 2008). All Participants that are not classified as Bank shall appoint a Settlement Agent. Notification of the appointment of a Settlement Agent shall be made in Writing to BoZ by both the Participant and the Settlement Agent.

The banks in Zambia are using technology as the driver for the business (World,2013). Since 1996, the Bank of Zambia has been reaffirming the importance of having a well-functioning payment that positively contributes to the financial stability of the country and the well-functioning of the country's economy (Payment, 2007). BoZ further states that a payment system is a system used to settle financial transactions through the transfer of monetary value and consist of the various mechanisms that facilitate the transfer of funds from one party (*the payer*) to another (*the payee*). Conversely, the Bank of Zambia realizes the important catalytic role that Digital Financial Services (DFS) can play towards the increased usage of electronic payment mechanisms by the general public (Matthew K. Luka, 2012).

The interest of network effect is significant in utilizing an Automated Teller Machines (ATMs) Kamyalile Simuchimba, BA (2011). Milne (2006) also encourages and supports the notion. Interestingly, Alhaji Abubakar Aliyu, Rosmaini Bin HJ Tasmin (2012) investigates the influence of the ICT evolution on the profit and cost effectiveness of the banking industry. Further (Alhaji Abubakar Aliyu, Rosmaini Bin HJ Tasmin 2012 states that similar in Kansas USA, Sullivan (2000) also found no systematic evidence that multi-channel banks in the 10th Federal Reserve District were either helped or harmed by having transactional web sites (Muhammad, 2013).

The use of ICT in the banking industry enables global economies to setup a financial system before first establishing a fully functioning financial infrastructure. Electronic banking to be cheaper and reduces processing costs for providers and less search and switching costs for consumers, banks can promote their services and products involving smaller transactions to lower-income borrowers, even in remote areas (Shirley J. Ho, 2006).

The modernization of ICT sets the stage for extraordinary improvement in banking procedures throughout the world. For instance, the development of worldwide networks has considerably decreased the cost of global funds transfer (Alawode, 2011). Banks that are using ICT related products such as online banking, electronic payments, security investments, information exchanges, financial organizations can deliver high-quality customer service delivery to customers with less effort (Stella E. Igun, 2014).

B. Governance in the banking Sector

Governance is defined as Establishment of policies, and continuous monitoring of their proper implementation, by the members of the governing body of an organization. It includes the mechanisms required to balance the powers of the members (with the associated accountability), and their primary duty of enhancing the prosperity and viability of the organization (C.L.Parmo, 2009). ICT and Security governance is a formal framework that provides a structure for organizations to ensure that IT investments support business objectives.

The board has not paid much attention to IT matters hence creating serious problems over the two decades, Information Technology has moved largely a support back-office to becoming the key enabler and enabler business (ITGI ,2008). IT is not only critical in its support of key business processes, but also transformational to the business at large. In a study conducted by PwC, it was found that while most organizations worldwide identify the importance of ICT and Security governance and most do not have a holistic view that considers all its dimensions (ISACA, 2006). The concept of ICT and Security governance as a main framework encompassing a wide spectrum of provisions, including the measurement of benefits, has yet to emerge. The alignment IT to the business objectives needs placed at the highest as a rated driver and desired outcome of ICT and Security governance practices (Ettish, 2017). The importance of IT alignment to deliver sustainable business results, and feel ICT and Security governance is one of the best means to achieve this (Michael Broudy, 2016).

The focus of ICT governance initiatives is still very narrow by focusing mainly on risk and control (Ettish, 2017). The initiatives are not considering ICT governance from a holistic perspective that can be used to enhance the value of IT for the organization. Without proper ICT and Security governance in banks, ICT systems can lose integrity with serious implications on the performance of a bank and can also result in a breach of client confidentiality (Rao, 2015).

C. Corporate Governance in the Banking Sector

A typical organization has corporate governance, IT governance and IT management is present. IT governance focuses on the IT-related areas within an enterprise corporate governance framework (Kan, 2003). Corporate Governance Is The Set Of Responsibilities And practices exercised by the board and executive management to provide strategic direction, ensure that objectives are achieved, while evaluating the risks applying appropriately controls and verifying that the enterprise's (N.C.Centre, 2005)resources are utilized effectively. ITGI (2009) notes that the terms „governance", „enterprise governance" and IT governance" may have different meanings to different individuals and enterprises depending on (amongst others) the organizational context (maturity, industry and regulatory environment) or the individual context (job role, education

D. IT Strategy in the Banking Sector

A strategy is defined as the direction an enterprise chooses to reach its goal. Goals are a description of the desired future condition, and strategy is the intentions of actions to realize the goals (N.C.Centre, 2005). The organisation strategy needs to consist of a set of main beliefs or formulas that are used to satisfy a company´s purpose (C.L.Parmo, 2009). These values are usually general directives for reaching some business goals. Strategies are plans that can be associated with project deployment and are defined from the overall business strategy, "Enterprise Architecture, IT Strategy and IT Governance (Orandi Mina Falsarella, 2017). An effective IT Strategy will benefit a company to achieve improved system solutions, from the upper management, precise resource estimations on IT-investments. An example IT Strategy covers the enterprise´s direction and strategy (mission, vision, goals, knowledge strategy), persons (competence needs), organization (future organization and control of the IT function), and an IT platform (computers, networks, databases, and applications) (CLARKE, 2014).

E. COBIT

COBIT 5 is a business framework for the governance and management of enterprise Information Technology (IT) (Pasquini, 2013). COBIT stands for Control Objectives for Information Business Process, and it is the invention of a global task force and development team from ISACA, a nonprofit, independent association of more than 140,000 governance, security, and risk and assurance professionals in 187 countries (ISACA, 2018).

COBIT aims at delivering value through good governance and management of information and technology (IT) assets to the stakeholders. Enterprise boards, executives and management are the stakeholders that have to embrace IT as part of the business and maximize value from the investment (ISACA, 2012). COBIT is an effective tool for managing external legal, regulatory and contractual compliance requirements interrelated to enterprise use of information and technology. COBIT 5 standard provides a complete framework that supports enterprises to achieve their goals and deliver value through functioning governance and management of enterprise IT (George, 2014).

COBIT 5 processes are split into governance and management areas. However, the two (2) process areas contain a total of 5 domains and are called principles. The COBIT 5 domains are broken down into 37 processes (Krishna Seeburn, 2014). COBIT 5 provides a comprehensive framework that supports the organization in realizing its business objectives for the governance and management of IT systems (Vyas, 2016). COBIT 5 enables IT resources to be governed and managed holistically, taking in a full end to end business processes in an organization.

METHODOLOGY

In Figure 1 we show our research design. The research was split between quantitative and qualitative research. Relevant published, Internet and unpublished materials aged less than 15 years were consulted in the study.

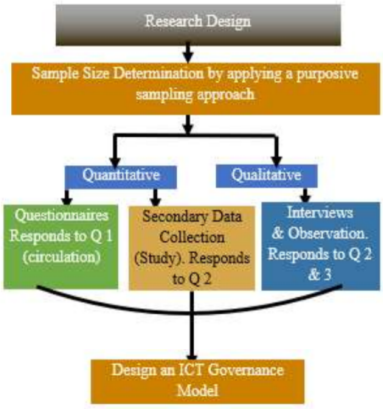

Figure 1. Research Design

A. SAMPLE SIZE

Data was collected from 37 participants from the 17 commercial banks. The research targeted a population of 255 and the sample size of 35 participant's working in the IT department for various commercial banks. The study was also done through direct observation and interview visits to various commercial banks

$$n_r = \frac{4pq}{d^2}$$

Where;

n_r = *required sample size,*

p = *proportion of the population having the characteristic,*

q = *1 – p and*

d = *the degree of precision.*

The proportion of the population (p) may be known from prior research or other sources; if it is unknown, use p = 0.5, which assumes maximum heterogeneity (i.e., a 50/50 split). The degree of precision (d) is the margin of error that is acceptable. Setting d = 0.1 0, for example, would give a margin of error of plus or minus 10%. Applying this formula to this research;

Since the researcher does not know, Gogtay (2010) recommends the researcher to assume = 0.5, and the value of q is = 1- p, d is to 90% accuracy; therefore

P = 0.5

q = 0.5 and d = 0.1, margin of error of ± 10%.

Therefore, the sample size is calculated with a confidence level of 90%, to be.

$$n_r = \frac{4pq}{d^2}$$

$$n_r = \frac{4 * (0.5) * (1 - 0.5)}{0.1^2}$$

The sample size is calculated with a confidence level of 90%, to $ben_r = 100$

The questionnaire was grouped into four (4) sections consisting of eleven (11) questions in total. The first section, Section A, Bio Data - Please tick in the box as appropriate; Section B General Information (Please tick as appropriate); Section C, IT Governance issues; Section D challenges may have hindered successful adoption of appropriate IT governance framework. Sixteen (17) commercial banks organizations with a sample size of 285 were targeted for the questionnaires with 39 respondents from 12 commercial banks responding.

A Likert scale was used to evaluate the level of agreement or disagreement with weights ranging from 1 - 5. This was used by respondents to evaluate the level of agreement or disagreement 5(100-80%),4(80-60%),3(60-40%),2(40-20%) and 1(20-0%) Percentages were used to find the level of agreement (sum of respondents for strongly agree and agree), disagreement (sum of respondents for strongly disagree and disagree), and neutral. The collected data were checked for completeness, and then coded, captured, and analyzed using Microsoft Excel. Descriptive statistics used included tables, frequencies, weighted mean, standard deviations, and percentages.

One of the limitations of this study is that it is highly dependent on the technical people who have hands-on experience in the field. Less than twenty individuals at each targeted organization in this research could provide complete and valid information, and the researcher relied heavily on interviews as a backup method of collecting data from the heads of departments to confirm that the data collected from the respondents were valid. Having an alternative method for collecting empirical knowledge could be a way to overcome this limitation. Other limitations are related to the scope of this study.

RESULTS AND FINDINGS

A. MATURITY OF ICT GOVERNANCE

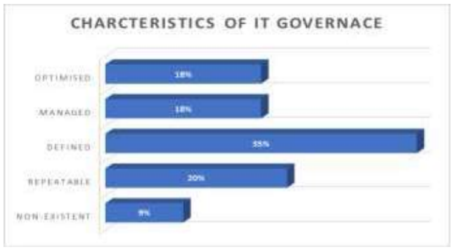

Figure 2. maturity level

Process Assessment Model tool was used to assess the maturity of ICT governance in the banks. on ISO/IEC 15504 process rating scale of (Not Achieved 0 to 15%; Partially 15% to 50% ; Largely Achieved 50% to 85% and Fully 85% to 100%). Therefore, the maturity of governance can be computed from ISO/IEC 15504 process rating scale by totalling 3 levels Defined (35%), Managed (18%)and Optimized (18%) and the total 71% . The computed 71% total falls between 50% and 85% on ISO/IEC 15504 process rating scale meaning that ICT governance is largely achieved but not fully achieved as per COBIT process as shown on figure 2 above.

B. LEVEL OF ICT GOVERNANCE

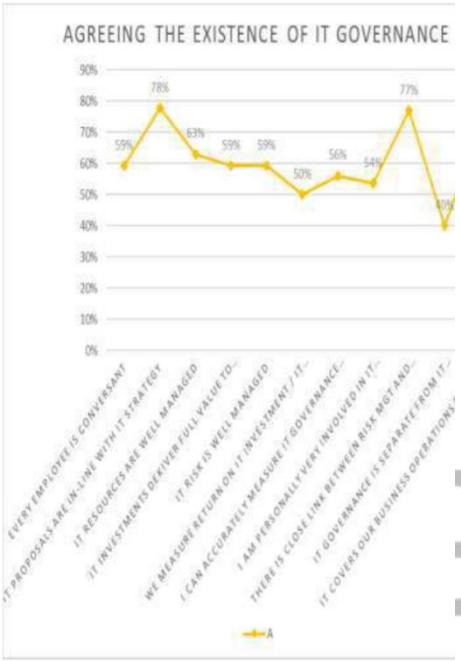

Figure 3. ICT governance level

As depicted from the figure above. ICT Governance level is above 50% except for the domain of separating management from governance. The level of governance was computed from ISO/IEC 15504 process rating scale of (Not Achieved 0 to 15%; Partially 15% to 50% ; Largely Achieved 50% to 85% and Fully 85% to 100%). Therefore, computing 50% in the scale meant that ICT governance is largely achieved but not fully achieved as the research also found that respondents were able to accurately describe ICT governance at their institution with a mean representation of 60%.

C. CORPORATE GOVERNANCE OF BANKS

Figure 4 shows the current corporate governance structure of banks in Zambia as far as ICT Governance is concerned.

As can be seen in Figure 4 all Banks do not have a Chief Information Security Officer.

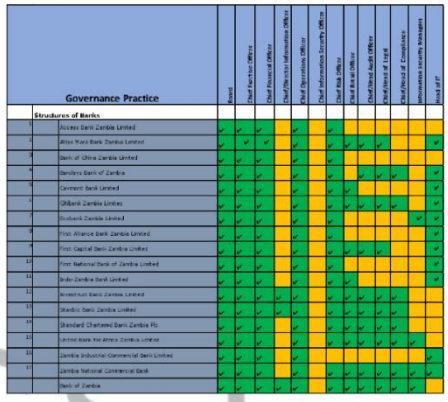

Figure 4. Corporate governance structure

Based on this finding shown in Figure 4, we are convinced that without a Chief Information Security Officer in any of the commercial Banks, it becomes impractical for any bank to implement or introduce Governance at ICT level as no one can take responsibility or ownership of this very critical role that ensures compliance with ICT governance.

To overcome, this challenge identified the study we recommend the solution or framework highlighted in figure 5.

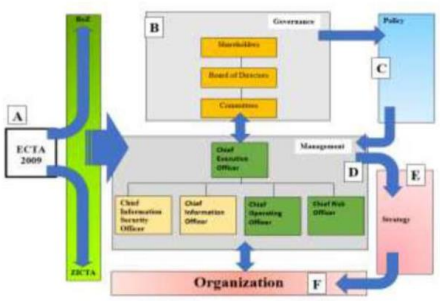

Figure 5. Proposed Bank Governance Structure Model

An explanation of this model follows. Sections highlighted by letters A – F shall be referred to as Module.

MODULE A: BoZ ACT

Through the guide of **ECTA [A]**, Central Bank (BoZ) issues a directive or ACT to compel the banks establish good corporate governance based on COBIT EDM01 process. The Board of Directors compels Management to include the Information Technology and Information Security in the Executive Management structure of the banks.

MODULE B: Governance

The proposed model bank governance aims at separating governance from management as per COBIT EDM01. Separating governance and management promotes accountability at all levels. In the context of the model, **governance** [B] is responsible for offering oversight and decision-making related to strategic direction, financial planning, and bylaws called the policies. **Policies [C]** are set of rules and laws that outline the organization's purpose, values, and structure. Governance provides a mechanism for good enterprise governance that focuses on stakeholder value by balancing performance and conformance. **Stakeholders** are the owners or shareholders and receives dividends when the organisation is making profit. Shareholders appoints the **Board of Directors** to oversight and strategic direction to Management through policies.

MODULE D: Management

Management [D] on the other hand, mainly involves controlling in alignment with the direction set by governance. The (executive) management team under the leadership of the **chief executive officer** or managing director is ultimately responsible for this. Again using the political system an illustration, it may imply the roles played by differing government parastatals, agencies and departments in Zambia. Management develops a **MODULE E** from the polices so that they may run routine decisions and administrative work related to the daily operations of the **MODULE F.**

CONCLUSION

In this paper we start by highlighting what banks do in Zambia and give a succinct explanation of the various elements of banking systems available and how they are run. We then showcase the ICT systems in use in Zambia and how these help banks to achieve their targets.

We have also shown the challenge at ICT Governance level for the banks in Zambia.

We have then concluded by showcasing the solution to overcome ICT Governance challenges in Zambia by showing our proposed framework of how the governance can be achieved. We hold the view that using this proposed model banks in Zambia can implement and achieve good corporate governance.

REFERENCES

[1] A. Mian, "Foreign, Private Domestic, And Government Banks:," *New Evidence from Emerging Markets,* p. 46, 2003.

[2] S. Heffernam, Morden Banking, John Wiley & Sons Ltd, 2005.

[3] E. B. M. Buckle, Principles of banking and fi nance, University of London International Programmes, 2011.

[4] L. E. a. A. Prizzon, A guide to multilateral development, odi.org, 2018.

[5] S. P. Krishna, ROLE OF CO-OPERATIVE BANKS IN FINANCIAL INCLUSION, SVPM's

College of Commerce, 2018.

[6] B. Act, "Co-operative Societies of the State and the finance and backing," p. 92, 2017.

[7] T. R. Dr.G.Tulasi Rao, "Role of Information Technology in Indian Banking Sector," vol. 17, p. 5, 2015.

[8] J. M. WESUTSA, "THE IMPACT OF ICT ADOPTION ON FINANCIAL PERFORMANCE OF," UNIVERSITY OF NAIROBI, 2010.

[9] S M Kundishora, "The Role of Information and Communication Technology ICT) in Enhancing Local Economic Development," South West Zimbabwe, 2008.

[10] Payment, "National Payment System Act," Bank of Zamabia, 2007.

[11] I. A. F. Matthew K. Luka, "The Impacts of ICTs on Banks," International Journal of Advanced Computer Science and Applications, 2012.

[12] M. S. S. I. a. M. A. Muhammad, "Information and Communication Technology and Bank Performance in Nigeria," Federal University Dutsinma, 2013.

[13] S. K. M. Shirley J. Ho, "The Impact of Information Technology on the Banking Industry," Queen Mary, University of London, UK, 2006.

[14] A. J. a. E. U. K. Alawode, "INFORMATION AND COMMUNICATION TECHNOLOGY," *International Technology, Education and Environment Conference,* p. 5, 2011.

[15] Stella E. Igun, "Strategic Impact of ICT on Modern Day Banking Nigeria," *International Journal of Strategic Information Technology and Applications,,* Vols. 5(4), 78-93,, p. 4, 2014.

[16] I. KOSKOSAS, "THE PROS AND CONS OF INTERNET BANKING: A SHORT REVIEW," *Business Excellence and Management, University of Western Macedonia, Kozani, Greece,* vol. 1, p. 10, 2011.

[17] A. A. i. Reixach, "The Effects of Information and Communication Technologies on the Banking Sector and the Payments System," Universitat of Girona, 2001.

[18] BoZ, "Annual Report Bank of Zamabia," Lusaka, 2004.

[19] ZECH, "Zambia Electronic Clearing House Rules," 2014.

[20] O. H. a. P. Esselaar, "Country Survey," 2003.

[21] T. Lammle, CCNA, Cisco Press, 2016.

[22] S. K. B. Yadhu Ravinath, "Backup Virtual Private Networks in Banks," *International Journal of Emerging Trends & Technology in Computer Scienc,* vol. 2, 2013.

[23] A. Agboola, "Information and Communication Technology (ICT) in Banking Operations in," Obafemi Awolowo University, 2007.

[24] S. S. M. K. a. K. Saadan, "The Formal Design Model of an Automatic Teller Machine (ATM)," *Lecture Notes on Information Theory,* vol. 1, p. 4, 2013.

[25] PwC, "Global Economic Crime and Fraud Survey," Pwc Zambia, Lusaka, 2018.

[26] M. R. a. V. K. T. By Niina Mallat, "Mobile Banking Services," *COMMUNICATIONS OF THE ACM,* vol. 47, p. 5, 2004.

[27] G. T. Krugel, "Mobile Banking Technology Options," p. 57, 2007.

[28] G. Anton, THE IMPACT OF INTERNET BANKING ON THE USE OF, Kyiv School of Economics, 2014.

[29] S. FIRDOUS, "IMPACT OF INTERNET BANKING SERVICE QUALITY ON CUSTOMER SATISFACTION," *Journal of Internet Banking and Commerce,* vol. 22, p. 17, 2017.

[30] R. A. H. A. A. B. Alshammari, "Analytical Study on Internet Banking System," *Jounal of*

Computing, vol. 2, no. 6, 2010.

[31] Y. A. a. A. Niaz, "The delicate balance of internet banking and bricks and mortar offices," Gotland University, 2010.

[32] B. o. Zambia, "NATIONAL PAYMENT SYSTEMS IN ZAMBIA," Bank of Zambia, Lusaka, 2015.

[33] O. O. Adeoti, "Challenges to the efficient use of point of sale (POS) terminals in Nigeria," *African Journal of Business Management,* vol. 7, no. pp. 2801-2806,, p. 6, 2013.

[34] O. A. K. Osotimehin, "Adoption of Point of Sale Terminals in Nigeria: Assessment of Consumers' Level of Satisfaction," *Research Journal of Finance and Accounting,* vol. 3, no. 1, p. 6, 2012.

[35] A. A. Ettish, "INTEGRATING INTERNAL CONTROL FRAMEWORKS FOR EFFECTIVE CORPORATE INFORMATION TECHNOLOGY GOVERNANCE," *Journal of Information Systems and Technology Management – Jistem USP,* vol. 14, no. 3, p. 10, 2017.

[36] I. G. Institute, "IT Alignment-Who-is-in-Charge," *IT GOVERNANCE DOMAIN PRACTICES AND COMPETENCIES,* p. 30, 2005.

[37] N.C.Centre, "A Best Pratice guide for Decision-makers in IT," *Internation Jounal ,* p. 22, 2005.

[38] C.L.Parmo, "Enterprise Architecture, IT strategy and IT governance," vol. 5, p. 151, 2009.

[39] C. A. S. C. J. Orandi Mina Falsarella, "Corporate Strategic Planning and Information & Communication Technology Planning: a project based approach," vol. 24, p. 12, 2017.

[40] J. CLARKE, IT Strategic Planning, From Australian Board and management Terms: ISACA, 2014, p. 90.

[41] F. M. S. R. C. S. C. M. S. Sabine Buckl, A Conceptual Framework for Enterprise Architecture Design, 2010.

[42] TOGAF, "Banking Industry Architecture Network & The Open Group," vol. 2, p. 20, 2012.

[43] M. S. K. Ahsan, "ROLE OF ENTERPRISE ARCHITECTURE IN HEALTHCARE ORGANIZATIONS AND KNOWLEDGE-BASED MEDICAL DIAGNOSIS SYSTEM," *JISTEM - Journal of Information Systems and Technology Management,* vol. 12, no. 2, p. 12, 2016.

[44] Jeff Tyree and Art Akerman, "Architecture Decisions:Demystifying Architecture," *Postmodern Software Design,* p. 9, 2005.

[45] S. S. &. S. Maguire, "Enterprise Architecture by Sparx Systems & Stephen Maguire," p. 6, 2017.

[46] Ramesh Radhakrishnan, "IT Infrastructure Architecture Building Blocks," *Sun Professional Services,* p. 27, 2004.

[47] B. Robertson, "Modeling Architecture and Infrastructure Planning:Domains to Patterns and Beyond," *Enterprise Planning & Architecture Strategies,* p. 23, 2002.

[48] A. Pasquini, "COBIT 5 and the Process Capability Model. Improvements Provided for IT Governance Process," *Obuda University Keleti Faculty of Business and Management,* p. 10, 2013.

[49] P. L. F. C. S. C. C. C. C. P. Krishna Seeburn, Basic Foundational Concepts, Student Book: ed., Mauricius, 2014.

[50] V. J. A. G. A. A. Y. Vyas, "Dubai Customs COBIT 5 Implementation," p. 6, 2016.

[51] M. D. Micheal Broudy, CISM Review Manual, 15 ed., ISACA, 2016.

[52] P. T. Joanne De Vito De Palma, "A Primer for Imlementing Governace of Enterprise IT," p. 52, 2016.

[53] G. F. Sona Karkoskova, "Extending MBI Model using ITIL and COBIT Processes," vol. 6, no. 4, p. 16, 2016.

[54] L. C. a. R. P. Mohanty, Understanding Value Creation: The Shareholder, 2007.

[55] A. Report, "REPORT OF THE AUDITOR GENERAL ON THE ACCOUNTS OF PARASTATAL," Auditor General, Lusaka, 2015.

[56] C. C. C. Debra Mallette, "Implementing COBIT® in your Organization," *San Francisco Chapter, Isaca,* vol. 12, p. 26, 2011.

[57] J. W. L. Le Thanh Trung, "Implementation," *COBIT® 5 Implementation,* p. 78, 2013.

[58] J. Pankaj Kumar Singh, Linking of Customer Satisfaction with Shareholders' value, Global Journal of Finance and Management, 2014.

[59] F. C. P. W. C. U. Paul A. Williams, IT GOVERNANCE DOMAIN PRACTICES AND COMPETENCIES, IT Governance Institute, 2015.

[60] A. S. George Mangalaraj, "IT Governance Frameworks and COBIT," *Mangalaraj et al.,* p. 10, 2014.

[61] S. L. Ndlovu, "Challenges of CoBIT 5 IT Governance Framework Migration," *International Conference on Information Resources,* p. 17, 2016.

[62] M. S. Z. MOHAMMED ALAA H. ALTEMIMI, "IT Governance Landscape: Toward Understanding the Effective IT Governance," *Scholedge International Journal of Business Policy & Governance,* vol. 12, no. 11, p. 13, 2015.

[63] M. S.-S. John Dooney, "How Centralized and Decentralized HR Department Structures," *the Society for Human Resource Management ,* p. 10, 2016.

[64] O. Onifade, "Seven COBIT 5 Implementation Pitfalls to Avoid," *D,* p. 2, 2018.

[65] J. B. S. E. 1Karim Youssfi, "A Tool Design of Cobit Roadmap Implementation," *(IJACSA) International Journal of Advanced Computer Science and Applications,,* vol. 5, no. 7, p. 9, 2014.

[66] N. Okon, "HOW TO APPLY COBIT 5 IN GOVERNMENT: THE CBN STORY," p. 25, 2017.

[67] S. MacDonald and N. Headlam, Research Methods Handbook, Manchester: Th Centre for Local Economic Strategies.

[68] Microsoft, "Get a better picture of your data," Microsoft, 13 April 2018. [Online]. Available: https://products.office.com/en-us/excel. [Accessed 13 April 13].

[69] P. F. w. D. KAMBANGANJI, "PIA complaint procedure," 16 November 2015. [Online]. Available: http://www.daily-mail.co.zm/pia-complaint-procedure/.

[70] Google, "Policyholder," 19 Januaruy 2019. [Online]. Available: https://www.google.com/search?q=policy+holder&rlz=1C5CHFA_enZM807ZM808&oq=policy+holder&aqs=chrome..69i57.3034j0j4&sourceid=chrome&ie=UTF-8.

[71] AfLife, "Pensions and Insurance Authority Press Statement," 19 January 2019. [Online]. Available: https://www.aflife.co.zm/?p=2350.

[72] J. KAGAN, "Insurance," 29 January 2018. [Online]. Available: https://www.investopedia.com/terms/i/insurance.asp.

[73] K. NYATI, "Insurance firms should harmonise operations," 19 January 2019. [Online]. Available: http://www.daily-mail.co.zm/insurance-firms-harmonise-operations/.

[74] TanzaniaInvest, "Tanzania Insurance," 19 January 2019. [Online]. Available: https://www.tanzaniainvest.com/finance/insurance.

[75] Sanlam, "How to Claim," 19 January 2019. [Online]. Available: https://www.sanlam.com/tanzania/customerservice/Pages/how-to-claim.aspx.

[76] BreakThroughAttorneys, "AN OVERVIEW OF SETTLEMENT OF INSURANCE DISPUTES BY THE INSURANCE OMBUDSMAN IN

TANZANIA," 13 OCTOBER 2017. [Online]. Available: https://breakthroughattorneys.com/insurance-disputes-tanzania/.

[77] Soko, " Search Soko Directory Top Six Challenges Facing the Insurance Sector in Kenya," 18 September 2015. [Online]. Available: https://sokodirectory.com/2015/09/top-six-challenges-facing-the-insurance-sector-in-kenya/.

[78] M. W. Kiana, "University of Nairobi Digital Repository," October 2010. [Online]. Available: http://erepository.uonbi.ac.ke/handle/11295/12619.

[79] Friss, "The 8 Biggest Fraud Challenges for Insurers," 19 January 2019. [Online]. Available: https://www.friss.com/press/the-8-biggest-fraud-challenges-for-insurers/.

[80] LusakaTimes, "Slow growth of insurance sector in Zambia worries Government," 15 January 2017 . [Online]. Available: https://www.lusakatimes.com/2017/01/15/slow-growth-insurance-sector-zambia-worries-government/.

[81] E. MSETEKA, "Liquidity problems hit insurance sector," 21 June 2016. [Online]. Available: http://www.daily-mail.co.zm/liquidity-problems-hit-insurance-sector/.

[82] DefinitionInsurance, "INSURANCE CLAIMS PROCEDURE IN KENYA," 2009. [Online]. Available: https://definitioninsurance.com/index.php/en/motor-insurance/list-of-insurance-claims-procedures/insurance-claims-procedure-in-kenya.

[83] h. A. S. Das, "LIFE INSURANCE, CHALLENGES AND OPPORTUNITIES IN RURAL INDIA," August 2017. [Online]. Available: https://www.researchgate.net/publication/319417319_LIFE_INSURANCE_CHALLENGES_AND_OPPORTUNITIES_IN_RURAL_INDIA.

[84] N. J. Gogtay, "Principles of Sample Size Calculation," *Principles of Sample Size Calculation* , pp. 517 - 518 , 2010 .

Questionnaire

The University of Zambia

School of Engineering

INFORMATION TECHNOLOGY GOVERNANCE IN ZAMBIAN COMMERCIAL BANKS

By Lemmy Mwanza (2016146017)

Master of Engineering – ICT Security

For further details or any queries, kindly get in touch on 0977 454850, lemwanzo@yahoo.com.

Dear Respondent,

I am a student at the University of Zambia in my final stage pursuing a Master of Engineering – ICT Security. As partial fulfilment for the award of a Master's degree, I am conducting a baseline study on: **"INFORMATION TECHNOLOGY GOVERNANCE IN ZAMBIAN COMMERCIAL BANKS."**

You have been purposively sampled to provide information for the topic indicated above. The information being collected is purely for academic purposes as such, it will be treated with

maximum confidentiality. Subsequently, you are not supposed to indicate your name or any personal information that can lead to revealing of your identity.

Your co-operation will be greatly appreciated.

For more information queries in relation to the survey, you may wish to contact the following:

Research Supervisor: Dr. Dani E. Banda (Daniel.banda@ymail.com) or

Assistant Dean: Dr. Erastus Mwanaumo (erastus.mwanaumo@unza.zm)

Part A: Bio Data - Please tick in the box as appropriate

1) **Gender:** **(a**) Male ☐ (b) Female ☐

2) **Age in years.**

(a)	18 – 22	☐	(d) 30 – 34	☐
(b)	22 – 26	☐	(e) 34 – 40	☐
(c)	26 – 30	☐	(f) 40 and above	☐

3) **Marital status**

(a) Single ☐
(b) Married ☐

4) What is your level education?

☐ Secondary
☐ Certificate
☐ Diploma
☐ Degree
☐ Master's degree
☐ PhD

Others specify……

5) Do you work within the ICT department or are apprised with ICT?

☐ Yes
☐ No

Part B: General Information (Please tick as appropriate).

6. Classify ownership of the commercial bank where you work?

( ) Local ( ) Foreign ( ) Both

7. How many local branches do you have?

( ) 1-5 ( ) 6-10 ( ) 11-25 ( ) 26-50

8. How many years has the bank been in operation?

( ) 1-5 yrs

( ) 6-10 yrs

( ) 11-25 yrs

( ) 26-50 yrs

( ) Above 50 years

9. What is your designation level?

( ) Board of Director

( ) Executive Management

( ) Chief Information Officer

( ) Business Unit Executive

( ) Other ……

PART C: IT Governance issues

10. How often does IT strategy Committee meet?

( ) 2-3 times a month ( ) Monthly ( ) Quarterly ( ) annually ( )Never

11. Does the board reviews IT budgets and plans on regular basis ( ) Yes ( ) No

12. We have structured processes to govern the following (Tick as appropriate)

( ) IT Assets

( ) Contracts or Master Service Agreements

( ) Service level Agreements and Operational Level Agreements

( ) All of the above

( ) None of the above

13. a. Does your bank follow a standard IT process governance framework e.g COBIT,VALIT,ISO/IEC 17799:2005?

( ) Yes ( ) No

c. If No in a. above, are you considering adoption?

( ) Yes ( ) No

9) Which of the following best characterizes IT governance at your bank?

( ) Non-existent: The banks have not recognized the need ( ) Initial: The processes are informal and uncoordinated.

( ) Repeatable: The processes follow a regular pattern.

( ) Defined: Processes are well documented and communicated.

( ) Managed: Processes are monitored and measured.

( ) Optimized: Best practices strictly adhered to and there are provisions for amending

10) How do you measure the effectiveness of IT governance strategies within your organization? a) Benchmarking

b) Use of a capability maturity models (e.g. CMM)

c) Other.....

11. How would you assess your bank based on the following best practices?

Issues	Strong agree (5)	Agree (4)	Neutral (3)	Disagree (2)	Strongly Disagree (1)
Every employee in your department well conversant with the banks IT strategy?					
Our IT proposals are in line with the approved IT strategy					
Our IT Resources are well managed					
Our IT investments deliver full value to the business					
IT Risk is well managed					
We measure return on IT Investment/IT Assets					
I can accurately describe IT governance at my institution.					
I am personally very involved in IT governance practice at my institution					
There is a close link between risk management and achievement of business objectives in our bank					
IT Governance is separate from IT management					
IT covers our business operations end to end					

PART D:

12) What challenges may have hindered successful adoption of appropriate IT governance framework;

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

Lack of enough institution to train on IT strategy issues					
Lack of clear understanding of IT Governance					
Lack of skilled personnel to impact the knowledge					
Lack of established metrics to assess level of IT governance					
Absence of documentation of IT strategies in our bank					
Lack of clear communication strategies					
Lack of project ownership					
Lack of working concept and knowledge by the board and executive management on issues related to IT governance					

Other reasons

_____

_____

_____

COBIT 5 Process reference

Align, Plan and Organise

AP002 RACI Chart

Key Management Practice	Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Business Executives	Business Process Owners	Strategy Executive Committee	Steering (Programmes/Projects) Committee	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information Security Officer	Architecture Board	Enterprise Risk Committee	Head Human Resources	Compliance	Audit	Chief Information Officer	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
AP002.01 Understand enterprise direction.		C	C	C	A	C	C				C	C		C				R	C	R	R		R	R	R	
AP002.02 Assess the current environment, capabilities and performance.		C	C	C	R	C	C				C					C	C	A	R	R	R	C	C	C	C	
AP002.03 Define the target IT capabilities.		A	C	C	C	I	R		I		C		C			C	C	R	C	C	C	C	C	C	C	
AP002.04 Conduct a gap analysis.					R	R	C				C				C	R	R	A	R	R	R	R	R	R	C	
AP002.05 Define the strategic plan and road map.		C	I	C	C		C		R		C	C				C	C	A	C	C	C	C	C	C	C	
AP002.06 Communicate the IT strategy and direction.	I	R	I	I	R	I	A	I	I	I	I	I	I	I	I	I	I	R	I	I	I	I	I	I	I	I

AP002 Process Practices, Inputs/Outputs and Activities

Management Practice	Inputs		Outputs	
AP002.01 Understand enterprise direction. Consider the current enterprise environment and business processes, as well as the enterprise strategy and future objectives. Consider also the external environment of the enterprise (industry drivers, relevant regulations, basis for competition).	**From**	**Description**	**Description**	**To**
	EDM04.01	Guiding principles for allocation of resources and capabilities	Sources and priorities for changes	Internal
	AP004.02	Innovation opportunities linked to business drivers		
	Outside COBIT	Enterprise strategy and enterprise strengths, weaknesses, opportunities, threats (SWOT) analysis		

Activities
1. Develop and maintain an understanding of enterprise strategy and objectives, as well as the current enterprise operational environment and challenges.
2. Develop and maintain an understanding of the external environment of the enterprise.
3. Identify key stakeholders and obtain insight on their requirements.
4. Identify and analyse sources of change in the enterprise and external environments.
5. Ascertain priorities for strategic change.
6. Understand the current enterprise architecture and work with the enterprise architecture process to determine any potential architectural gaps.