AN INVESTIGATION INTO CYBER SECURITY THREATS POSED BY INSIDERS: A CASE OF PUBLIC ORGANISATIONS

By

MELISSA KAEMBY CHINYEMBA

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

THE UNIVERSITY OF ZAMBIA

LUSAKA

2019

DECLARATION

I, **Melissa Kaemby Chinyemba**, hereby declare that this submission is my own work and that, to the best of my knowledge and belief, it has never been produced or submitted previously at any university or other institutions for academic purposes and agree that similar studies have been done but not exactly the same as this. All source of published materials used has been duly acknowledged.

Author

Melissa Kaemby Chinyemba

Signature: ….……..…….. Date:…../……/ 2019

Supervisor

Dr. Jackson Phiri

Signature: ….……..…….. Date:…../……/ 2019

APPROVAL

This dissertation by Melissa Kaemby Chinyemba is approved as partially fulfilling the requirements for the award of the Master of Engineering degree in Information and Communications Technology (ICT) Security of the University of Zambia.

Examiner 1: Dr. Simon Tembo Signature: ……..…….. Date:…../……/ 2019

Examiner 2: Dr. Dani Eliya Banda Signature: ……..…….. Date:…../……/ 2019

Examiner 3: Dr. Luka Ngoyi Signature: ……..…….. Date:…../……/ 2019

Chairperson Board of Examiners: Dr. Michael N. Mulenga Signature: ……..…….. Date:…../……/ 2019

Supervisor: Dr. Jackson Phiri Signature: ……..…….. Date:…../……/ 2019

DEDICATION

This dissertation is dedicated to my princess, Mirriam Lissa Mutakwa, I deprived you of the joy and pleasures of being a mummy as I opted to be with books in all my free times, and yet you still made my coffee and gave me that lovely smile as you encourage me to take a rest. You splash me with joy and happiness every day, and your beautiful smile melts my heart. This is for you my baby to surpass.

My nephew and son Daniel Chinyemba who have dared to follow my footprints, as you embark on your Computer Science journey, mummy has paved a way for you to surpass, and here you go.

My baby sister and eldest baby of the house Elizabeth Mahongo Chinyemba, your efforts in sorting the box of questionnaires by putting them in one place and forever making my cup of Kasama coffee has yielded this and it goes to you. You are simply amazing.

My big Brother and best friend, Arnold K. Chinyemba, your pride in the woman I' am and extraordinary patience when you came to see me and I was so busy with books nearly ignoring you, yet you still waited for me quietly as ever, till I got done. You are simply the best brother one can ever ask for in the whole universe. Here is a reward for your love.

Queen mother, Rhodah Ngambo Chikanda Chinyemba **aka** Mama nya Kasoko, your love is simply amazing. Your prayers, guidance, care, pride, patience and a listening ear to my never-ending demands is just breath-taking. You are indeed a mother and a half, the best mother a child can ever have. Forever supportive, protective and generous. Long live mum as we bless you with more achievements.

My family; aunties, uncles, sisters and cousins, you people were a backbone of steel when everything seemed unbearable and I could not contend. Your standing still with me in prayers, encouragement and support made this work a success.

To my heavenly father, everything works together for good to those who love the Lord. Thank you Lord for your sustenance and sovereignty, you are almighty God!!! .

ACKNOWLEDGEMENTS

One of the great pleasures of making such a research project a success is acknowledging the efforts of many people whose names may not appear on the title page, but their effort, cooperation and understanding were crucial to the fruition of this study.

First thing first, I thank God for the gift of life and the grace that he has imparted in me through my MEng ICT Security studies at the University of Zambia. He held my hand, walked with me and sustained me. Daddy, you are a sovereign God.

Sincerely, I would like to convey my heartfelt gratitude to **Frank L. Chibesakunda, Manager ICT Security ZESCO Ltd**. for his unprecedented interest, support and guidance for my academic progression. May the good Lord remember your generosity.

Very Special thanks go to the following who contributed to the better and wiser Cyber Security Professional I am today:

i. **Dr. Jackson Phiri** my research supervisor, for your valued guidance and evaluating my work. You patiently guided me through each step up to the completion of this study. You exposed me to the Deep web, hacking tools, Information security and Data privacy, this has been so useful for my research. May the good God richly bless you.
ii. **Dr. Erastus Mishengu Mwanaumo**, your support, updates and check-ups on the progress of my research, can never go unappreciated.
iii. **Dr. Collins C Kachaka,** I learnt a lot from you on Cyber readiness in Zambia and your efforts cannot go unappreciated.
iv. **School of Engineering:** Members of staff am grateful for the support through the times I spent under your care as a student. My schoolmates, MEng ICT Security class of 2017- 2018, thanks so much for the friendship and love, you guys are indispensable and simply the best.
v. **Public Sector:** Chief Executive Officers (CEO's) from Zambia's various Public organisations, this study would have never been a success without your support and your commitment can never go unappreciated.

Matthew Ndhlovu, my dear you have had so much faith and pride in the woman I' am and you have stood by me even on times that I got so busy to chat with you. Here is a reward for your endurance.

To my spiritual fathers, Rev. Kangwa Mumba and Big Dad, Bishop Joe Imakando, for your spiritual guidance, encouragement and proud parents of a daughter I' am, this is for you.

ABSTRACT

Insider attacks are the most hazardous threats faced by most organisations today and is an overwhelming task to deter, because employees require legitimate access privileges to organisational resources for their daily tasks. If they misuse this trust accidentally or intentionally, it can compromise data security, thereby, negatively impacting the corporations' reputation and revenue. Most Zambian public organisations have continuously been caught unaware on how their confidential information has ended up in the public domain. This is because most of these organisations have neither adopted nor fully implemented any of the security standards or frameworks such as Control Objective for Information and related Technology (COBIT) and or International Standards Organisation (ISO) 27000. The study established a theoretical model from ISO 27001 controls literature that analysed the Information and Communication Technology (ICT)/Cyber gaps for organisational cyber readiness. Using Actor-Network Theory (ANT) and Theory of Planned Behaviour (TPB), the study established the types of vulnerabilities that can be exploited by insiders and evaluated the effectiveness of the current controls in public organisations. Further, the study carried out a gap analysis using ISO 27001:2013 to understand the security gaps that relates to insiders so as to be able to propose an insider threats mitigating model with a core focus on user awareness and access control. The approach to this study was both quantitative and qualitative research. Questionnaires and interviews were used as an assessment tool for empirical study. The targeted population was the ICT/Cybersecurity Stake holders in public organisations that included; Executive Management, ICT/Cyber Security, ICT, Human Resources (HR), Legal, Enterprise Risk Management (ERM) and Internal Audits staffs, applying a convenient sampling method for participant identification. Microsoft-excel and SPSS were used for statistical analysis. All the three objectives of this study were achieved. The findings showed that, out of a total of eight public organisations under study only 25% had adopted international security standards and frameworks though partially implemented. The other 25% have adopted some security base practices while 50% have no security measures in place. The findings also revealed that most public organisations lack key ICT/Cyber Security policies and procedures. Additionally, the current controls are not effective enough to deter cyber security threats by insiders from exploiting their employers. Further, the findings yielded a useful model for mitigation of insider Cyber Security threats and highlighted relationships between management involvement, organisational Cyber Security values and the Cyber Security culture in public organisations. The significance of this study is to enforce cyber readiness in public organisations with an aim of enhancing insider data security mechanisms through the use of user awareness, access control, underground screening and Non-disclosure agreements (NDA).

Keywords: *Insider, threats, Cybersecurity, Mitigation, risk, fraud, user-awareness, access-control Public Organisations.*

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST APPENDICES

ABBREVIATIONS

ANT	Actor-Network Theory
APT	Advanced Persistent Threats
CD	Compact Disc
DVD	Digital Versatile Disc
CERT	Computer Emergency Response Team
CEO	Chief Executive Officer
CFO	Chief Financial Officer
CG	Commissioner General
CIA	Confidentiality, Integrity and Availability
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CSIRT	Computer Security Incident Response Team
COBIT	Control Objective for Information Related Technology
DG	Director General
DLP	Data Loss Prevention (DLP)
DoD	Department of Defense
DON	Department of Naval
DPSRC	Defence Personal Security Research Centre
EY	Ernest and Young
FBI	Federal Bureau of Investigation
HR	Human Resources
IBM	International Business Machines
ICT	Information and communication technology
IT	Information Technology
IP	Intellectual Property
ITIL	Information Technology Infrastructure Library
IRP	Incident Response Plan
ISMS	Information Security Management Systems
ISO	International Standards Organisation
IoT	Internet of Things
KPMG	Klynveld Peat Marwick Goerdeler
MERIT	Management and Education of the Risk of Insider Threat
MD	Managing Director

NSA National Security Agency

NDA Non-Disclosure Agreements

NDRI National Defense Research Institute

IDS Intrusion Detection

IPS Prevention Systems

RBAC Role-Based Access Control

SANS SysAdmin, Audit, Network, and Security

SCADA Supervisory Control and Data Acquisition

SOC Security Operations Center

SIEM Security Incident and Event Management

SDLC Systems Development Life Cycle

SPSS Statistical Package for the Social Sciences

SLA Service Level Agreement

SLC Single Level Flash Cell

P/E Program/Erase

MLC Multi-Level Cell

TPB Theory Planned Behavior

UIT Unintentional Insider Threat

UK United Kingdom

USA United States of America

USB Universal Serial Bus

DEFINITIONS OF TERMS

Confidentiality	Shall mean ensuring that data and information is only accessible to authorised users
Integrity	Shall mean ensuring that the data and information being accessed, processed, transmitted or stored has not been tampered with, altered or damaged.
Availability	Shall mean ensuring that the data and information is readily accessible to the authorized users
ICT Security	Shall mean preservation of confidentiality, integrity and availability of ICTs
ISMS	Shall mean the overall management processes that take care of planning, implementing, maintaining, reviewing and improving ICT Security
Information Assets	**S**hall mean any data or information that has financial value
Software Assets	Shall mean authorized application and systems software
Insider Threat	Shall mean any former or current business stakeholder with legitimate access to the organisational resources who compromises the security of that resource, intentionally or unintentionally
Vulnerability	Shall mean any weakness that can easily be exploited

CHAPTER ONE

INTRODUCTION

1.1 Background

Cyber Security has become an integral part of both public and private organisation's business processes, in maintaining the Confidentiality, Integrity And Availability (CIA) of information, because Information And Communication Technology (ICTs) play an important role in business operations. Majority of organisations today can no longer be imagined without the underlying digital systems and technological infrastructure for information handling [1]. Information protection from unauthorised access and misuse, including resilience of the underlying ICT infrastructure to various sorts of attacks, has become one of the main technological challenges faced by business houses and organisations [2]. This is because ICT has become more prevalent and complex, meanwhile, the increase in the sophistication and volume of cyber-attacks are at an alarming rate [3].

Most of the organisations' Executives Management, have recognised the growing importance of Cyber Security by showing willingness to adopt various international standards and frameworks such as COBIT5.0, Information Technology Infrastructure Library (ITIL), International Standards Organisation (ISO) 20000, ISO 27000 and ISO 31000, in an effort to govern and manage information, communications and related technologies [4],[5]. However, ICT Risk Management related policies, procedures and base practices, which should predominantly govern the presence of an effective internal threat management program, are usually overlooked thereby leaving the insiders cyber risks unattended to, yet they are critical to business operations [6].

An **insider** is an existing or past stakeholder with unrestricted access rights to sensitive organisational resources, who with or without intent compromises the resource security [7].

A **threat** in information security can be any mischievous act that endeavors to attain illegal access to the infrastructure. Therefore, the duo gives us an Insider threat definition.

Insider threats are a progressive attack vector that requires much more than just technology to mitigate, but social-technological solutions due to the intricacy of both technology and human beings currently. These insider threats are defined as Intentional (Malicious) and Unintentional (non-malicious or accidental).

Malicious insider threats are categorized into three namely; Fraud, Information Technology (IT) Sabotage and Intellectual Property (IP) theft [8]. Basically, one does not become a malicious insider until they abuse their access rights and or commit a crime wilfully. They are simply an insider, however, it is worthy of probing the track that one might take from being an insider to malicious insider [9]. Some examples of malicious but non-targeted attacks by outsiders include viruses and worms. These are created without any specific target in mind but generally propagates as much as they can through compromising vulnerabilities that includes insider vulnerabilities with which they are designed to exploit [10].

Financial fraud: motivated by financial gains includes instances where an insider performs a crime and or uses the available system to unlawfully modify the organization's information for personal and financial gain. Fraud motivated by financial gain is often caused when insiders see a chance to make a profit by abusing privileges or when outsiders offer money to steal personal information for identity crime and or modify information [9], [11].

Sabotaging: motivated by revenge due to job termination and disillusionment of employees by certain corporate decisions that do not favour them, is when an insider directs specific harm at a system, an individual or organization resources due to various wilful reasons [9], [12]. Analysing Sabotage using Actor-Network Theory (ANT) and the Theory Planned Behaviour (TPB), it is deduced that sabotage is motivated by revenge and often caused by employees who become dissatisfied with the company's compensation, arguments, supervisors, co-workers, reprimands, or job termination.

Sabotage threat is usually executed by employees with high technical skills and access to critical assets, like ICT technologist, engineers and System Administrators [10], [13].

IP theft: motivated by competitive advantage involves instances where an insider uses the available system to steal proprietary information of an organization [3]. This can be when insiders steal property for a competitor or their own business. In the early 2000s all the way to 2004, IP theft from U.S.A companies due to espionage was predictable to be costing $250 billion per year, despite the fact that it wasn't specified as to what extent insider action contributed to the figures. Today the correct figure might not be known because most of the organisations do not realize when they have been compromised, and the majority of the few that are aware do not report the attacks for fear of losing customer confidence and competitive advantage [13].

Insider Risk Landscape

Insider threat mitigation is all about data security which is initiated by an endeavour to ensure the CIA of information. This risk landscape is concerned with a number of categories that includes internal employees among others, who later after abusing their lawful access rights becomes an insider threat [2]. This is represented in the triangular loop in Fig 1.1.

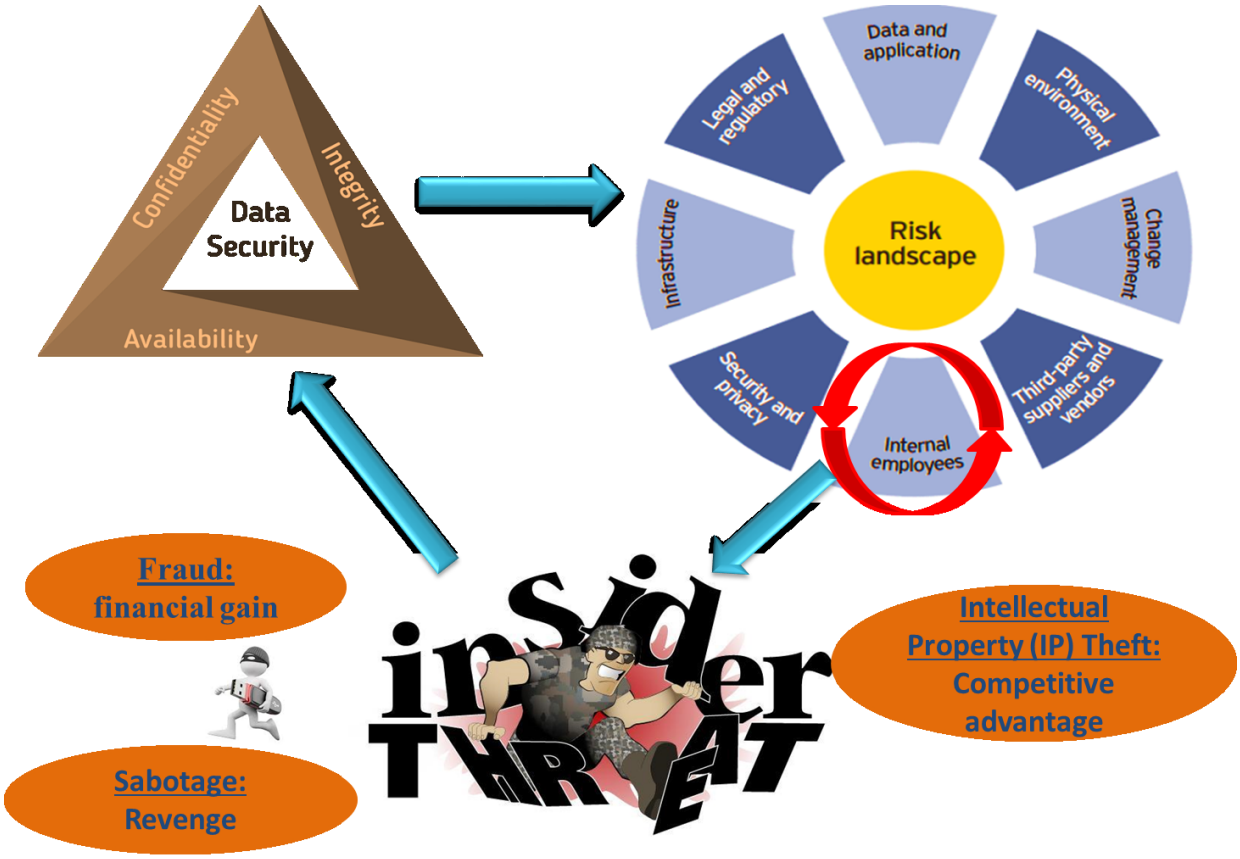


Fig 1.1: Insider threat landscape [2], [3], [14].

A vital note from the Computer Emergency Response Team (CERT) research states that it's prudent to look at these three crimes unconventionally and conspicuously because their nature, as well as the mechanism for detection and prevention, can be diverse. For instance, about 24% of IT sabotage incidents are usually committed by system administrators and engineers mostly after termination of contracts, whereas 16% of IP theft incidents are usually committed by those whose job, once had something to do with that IP then 44% of Frauds are normally committed by lower management employees such as service desk, frontline and or customer services personnel [9].

The CERT states that non-malicious insiders cause ICT security incidents accidentally for different reasons that include; human error, lack of user awareness, drugs, fatigue, stress, moods,

gender issues, drugs, age and or cultures. These accidental threats are referred to as "Unintentional Insider Threat (UIT)" the most common examples includes security incidents such as excessive access rights being granted to wrong users, introducing vulnerabilities during software development when Systems Development Life Cycle (SDLC) steps are bypassed, leaving an unencrypted portable storage device unattended to, system configuration errors, inactivating security controls, voluntary rule breaking, self-benefiting without malicious intent [15]. These are insiders who can cause damage to an organisations resources by their actions unintentionally. Verizon reported that from a comprehensive collection of security incidents, 14% were committed by insiders, while digital guardian reported that insider attacks account for 59% of the incidences [16]. Despite the fact that majority of them were of a deliberate and malicious nature, there still is a substantial impact from unintentional acts such as sending sensitive documents to a wrong recipient, as well as less-frequent mistakes by system administrators and programmers[16].

Insiders both malicious and non-malicious can motivate the success of these non-targeted malware exploits in various ways that include, exposing the organisation in social engineering attacks, being a doorway of malware onto the network by using infected removable storage media, opening unsafe attachments and or visiting hostile websites [9]. They are capable of incidentally putting the organisational information at risk due to the fact that the accepted work processes they operate, are risky or simply because there are neither right tools in place nor the right awareness training provided. For instance, it may be a common practice that employees put alternative email addresses on their business cards and also carbon copy their work to themselves on these consumer-grade web-based email systems including Yahoo, Icloud, Hotmail or Gmail. They can also share documents with others using personal storage solutions like Google Drive, Evernote, Icloud, Dropbox. These personal Internet hosted systems take the organisational resources beyond the system of control which can put it at risk of compromise [9].

Majority of the implementations of Information Security Management Systems (ISMS), such as ISO 27001, are conventionally focused on preventing external attackers by protecting the digital perimeter, access management, policy compliance and managing vulnerabilities [17], [18]. Recent surveys showed that internal fraud risks, being an area that has long been managed using forensic data analytics, had been ranked as the top use case at 77%. While Cyber breach and sabotage is ranked the second-highest risk area use case at 70% [19], [20]. Therefore, it is common knowledge that internal attackers generally accounts for approximately more than half of the risks that an organisation is exposed to whilst the external threats account for approximately above a third of the risks despite the gravity of the external consequences to an organisation [19].

With the above insider threat highlights, it was sort prudent that an investigation into cyber threats posed by insiders in public organisations be carried out to ensure that a cheap and sustainable mitigation model be of high priority for all organisations, structured with Executive Management's support demonstrated by approval of policies, procedures, standards and controls. This is because, advanced intelligence-led security, against Advanced Persistent Threats (APT) as well as customary security, have proved to be futile against insiders due to its complexity [20].

All employees have a degree of trust invested in them by their employers and have been granted physical and logical access to the organisation's ICT's, in order to fulfil their daily duties. Most of these employees are gratefully honest, however, there also exists the risk that some will abuse their inside position to commit crimes against their organisations [21]. A good example is a case of USA Army soldier Bradley Manning who in his role as an intelligence analyst, leaked through WikiLeaks organisation, the largest set of classified documents and videos to the public ever in the history of United States of America (USA) Military Army [22]. These threats can take the form of a malicious employee downloading sensitive or confidential information and divulge to the public domain, or an unhappy employee destroying data before quitting. In April 2008, an insider at the Sumitomo Mitsui Banking Corporation in London gained access to the bank's computer network in an attempt to pull off what would have been the biggest bank theft in the United Kingdom (UK) [23].

Insider Crimes: The probable impact of an insider crime ranges from trivial irritant to the disastrous in ratio, which can feasibly have an outcome of bankruptcy, death, regulatory contempt, environmental adversity, countered weapons systems, damage of reputation, loss of customer confidence, incurred legal costs, collapsed stock market among others [24].

Management and Education of the Risk of Insider Threat (MERIT) and Defence Personal Security Research Centre (DPSRC) records various insider attack vectors' incidences in their database of insider incidents maintained with related research conducted by Computer Emergency Response Team (CERT) which has numerous entries from public sources, collected since 2001 for misuse of organizational information by potential insiders includes but not limited to printing, emails, copiers, web posts, blogs, and social media chats and many more that includes the following [23], [24], [25], [26];

1) WikiLeaks - The case for USA Army soldier Bradley Manning who in his role as an intelligence analyst, leaked through WikiLeaks organisation, the largest set of classified documents and videos to the public ever in the history of USA military.

2) Supervisory Control and Data Acquisition (SCADA) - In a case of an electrical supervisor who developed an application for a SCADA system which was being used by the water firm. He installed a malicious programme on one of the organization's critical systems, after his contract termination, and damaged the SCADA system.
3) Cell Phone Clones - In a case of a group of insiders at a wireless telecommunications company who cloned more than 16,000 customer cell phones. The insiders made approximately $15 million worth of unauthorized calls for a period of six months.
4) POS System - In a case of a secretary who worked at a youth organization for over 20 years used a point-of-sale system to issue at least 500 fraudulent refunds totalling over $300,000 to the insider's own bank account over a 5-year period.
5) Banking - In a case of a manager for a branch of a banking institution who stole over $225,000 from business accounts after running into family health problems, gambling and unforeseen expenses.
6) Copier - In a case of Sheldon Boon, an Army signals analyst for National Security Agency (NSA), who used a handheld scanner to copy 52 classified documents and later passed to the Soviets.
7) Emails – In a case of a naturalized U.S.A citizen from the Philippines, while working at the Federal Bureau of Investigation (FBI) took and transferred classified information to senior political officials of Philippines in an attempt to overthrow that country's government.
8) Printing - In a case of a Robert Chaegun Kim, working for the Naval Intelligence removed classification label and printed the `secret' and `top secret' government documents.
9) Classified information Leakage - In a case of a University Professor who was charged with relaying sensitive information to China, and in one instance had sensitive files e-mailed to himself while in China.

The insider crime is a single name jacketing a variety of different threats. In practice to date no single method has proved prevailing as a solution, hence the importance to consider any solution space as likely combining elements of prevention, detection and response against the acknowledged insider attack types using both technical and sociological mechanisms that Zambian public organisations can leverage on in the fight against cyber insiders[24].

1.2 Rationale of the Study

In the recent past, organisational insider attacks have grown exponentially. For instance, in 2007, a study by Klynveld Peat Marwick Goerdeler (KPMG) revealed only 4% of the total recorded cyber incidents were instigated by malicious insiders [26]. Three years later the figure increased to 20% and 2013, Verizon's extensive review stated that 69% of information security incidents were ascribed to insider threats [16]. The growing dimension of threats to insider can be evidenced by the revolution of the internet and the growth of the Internet of things (IoT). However, knowing what exactly motivates inside threats is the right path to finding a strategic solution of how to mitigate the problem to an acceptable level [16].

One of the well-known insider related cyber-attacks of a growing spectacle involved Target in 2013, in which 40 million customers' credit card number and about seventy (70) million of personal data were stolen by cybercriminals. This incident saw the Chief Information Officer (CIO) and Chief Executive Officer (CEO's) out of employment as well as company reputation for competitive advantage [29]. The worst case scenario is that, despite the fact that the perpetrators were outsiders, they accessed the system using credentials of an insider who was one of the organisations' refrigeration's vendors [30].

Considering the fact that every business house has its trusted employees, business associates, contractor, vendors and all related stakeholders, with whom corporations do business with and are given access to the systems, it is a high opportunity. If these insiders not well managed, they may cause so much damage or harm to the corporation. According to a review of the danger from within by Harvard Business review, it is clear that most organisations admit that they don't have enough security controls to detect, prevent and mitigate insider attacks due to the fact they are yet to accept the degree of the Risk. Insider threat which is motivated by the technology complexity and Internet of Things (IoT) as stated above is growing by the day and cannot be left unattended [30].

It is against this background that ensuring a cheap and sustainable insider mitigation model for public organisations in Zambia would lead to improved data privacy and national cyber readiness.

1.3 Problem Statement

Having highlighted the challenges associated with detection, identification and mitigation of insider threats in business operations and public organisations, backed by the number of researchers who have laboured so much in the past in search of the solutions to mitigate insider

threats from various countries, proves that insider threat is a global problem that requires considered efforts to mitigate and Zambia is not an exception. Fig 1.2 shows the various recorded insider perpetrated information leakage in Zambia's public sector alongside the catalysts [31], [32].

Fig 1.2: Consolidated insider problems in Zambia

The assertion of the problem statement for this research, therefore, reads as follows:

'Most public organisations in Zambia have continuously been caught unaware on a number of occasions, how critical and confidentially classified matters have ended up in the public domain'.

1.4 Aim of the Research

The aim of this study is to investigate Cyber Security threats posed by insiders and enhance insider threat mitigation controls in public organisations focusing on the challenges and solutions thereby securing critical data.

1.5 Research Objectives

The objectives of this research are the following:

i. To determine the types of vulnerabilities in public organisations that can be exploited by insiders
ii. To establish the effectiveness of the current controls in public organisations in protecting against potential Cyber Security threats from insiders

iii. To design and propose measures to mitigate insider threats.

1.6 Research Questions

This research focused on answering the following questions:

i. What types of vulnerabilities can insiders exploit in a public organisation?
ii. How effective are the current controls in mitigating the Cyber Security threats from insiders?
iii. Is it possible to recommend mitigating measures to insider threats that address the issues in question (i) and (ii) above?

1.7 Scope of the Research

The study investigated into the current Cyber Security threats posed by insiders in Zambia's public organisations based on ISO27001: Information Security Management System (ISMS) standard, anything away from ISO27001, insider threats and public organisations is out of scope.

1.8 Significance of the Study

This study is significant in that it creates an understanding and appreciation of the importance of Cyber Security threats posed by insiders in Public Organisations and tailors the approach to internal threat mitigation so as to ensure data Confidentiality, Integrity and Availability (CIA). More so, this study is important because:

i. To enhance cyber readiness in public organisations for economic development, there is a need to tailor insider threat mitigation as a means to avert potential insider risks and ensure data security
ii. This study is the first of its kind in Zambia and will contribute to the body of knowledge mastery in this area.
iii. Security is said to only be as strong as its weakest point which is the internal employees known as insiders [33].

1.9 Research Constraints and Limitations

Due to the sensitivity of the research topic, most public organisations required that permission be sought from the Chief Executive Officers (CEOs), Director Generals (DGs) and Line Directors to grant authority to the researcher for data collection, needless to say, these are the most busy offices

that reaching out to them and awaiting their approval was very difficult and time consuming. The above factor including financial limitation and time constraint led to the fact that despite the sample selection including Top or Executive and Middle Management from Public Organisations, only eight organisations headquartered in Lusaka were considered in this study. These eight public organisational sectors included; Finance, Banking, Energy, Higher institution of learning, Government Agencies as well as Authority and regulatory boards. However, it is important to mention that all the necessary sampling procedures and techniques were followed to avoid bias and that the findings and solutions proposed are applicable to any other public and or private organisation that utilises ICTs for their day to day operations.

1.10 Organisation of Dissertation

This dissertation contains six chapters organised in the following order:

First Chapter gives an introduction to the research. It gives an overview of the study, the rationale, outlines the research problem and justifies the research. It further states the research objectives, research questions, scope, the significance of the study and research constraints.

The Second Chapter looks at the background literature and the related studies which meet the objectives by comparing and contrasting the previous works of other researchers and provide support for the development of the proposed Insider cyber threat mitigation model to reduce the risks associated with insider threats to an acceptable level.

The Third Chapter presents the methodology adopted for this study. It kicks off by discussing the research approach, design and targeted population. Thereafter, the sample size, sampling processes as well as justifications that were employed before considering data collection approach, instruments, methodological reliability and validity of various techniques used in this study.

The Fourth Chapter presents the actual findings and results of the data presentation as obtained during the data collection. This aimed at fulfilling all the three research objectives which were looking at investigating the public organisations' Cyber Security threats posed by an insider as well as determining the effectiveness of the current controls particularly to do with protection against internal Cyber Security threats

Fifth Chapter Five discusses and analyses the findings of the previous chapter in details as they relate to the objectives in relation with the existing body of knowledge on the subject matter of Insider Cyber threats in public organisations.

Finally, the chapter concludes the thesis by providing the conclusion and recommendations of the research based on the literature review, findings and analysis in line with the objectives and research questions for future studies in the same area.

1.11 Chapter Summary

This chapter introduced the study by looking at the core prerequisites of the research as presented in the research background, problem statement and justification. It further highlights the rationale, aim, objectives significance, scope and constraints of the study. Finally, we formulate the hypothesis and highlight the organisation of thesis.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

Organisations today continue to suffer significant damage due to breaches, which has caused a swing in the security perception from the traditional perimeter defence to a holistic understanding of the organisational exposure to threats and the causes of the breaches [34] Despite the fact that most of the breaches are from outsiders, insider threats can cause unimaginable harm to the organisation. Most studies and surveys show that organisations are now becoming cognisance of the dangers and harm that insider threats can cause and the importance of protecting against them. There are several factors affecting Insider threats in organisations due to the intricacy of technology coupled with human factor [7].

Therefore, in an effort to meet the third objectives which aim at developing and formulating a hands-on internal threat mitigation model to reduce the risks associated with insider threats to an acceptable level, related works had to be reviewed. This chapter reviews related fiction for the advance of the study's research model from various sources like journals, conference papers, reports, textbooks, government documents coupled with selected items from the internet, which serves as the foundation of the research. For us to develop the model for this study, it was vital to consider the reviewed literature contents and start by establishing various definitions related to Information security, the insider threats and the categories. Then defining how the insider threats come about (the drivers), what indicators review the insiders at work, insider threats detection, prevention and response, the consequences of insider attacks, mitigation model, the insider threat program and components of a successful mitigation program. This chapter aims at drawing valuable lessons relevant to this study form the existing body of knowledge on the subject.

2.2 Definition of Information Security

An ANSI Federal Standard 1037C glossary of telecommunications terms defines information security as "the protection of information against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional" [35]. Meanwhile the U.S. Department of Defence (DoD) defines information security as "the system of policies, procedures, and requirements established under the authority of Executive Order 12958, 'Classified National Security Information' to protect information that, if subjected to unauthorized disclosure, could reasonably be expected to cause damage to the national security" [36]. Chief Security Officer

Magazine defines information security as: 'The process of protecting data from accidental or intentional misuse by persons inside or outside of an organization. Although information security is by no means strictly a technical problem, its technical aspects (firewalls, encryption and the like) are important. Information security is an increasingly high-profile problem, as hackers take advantage of the fact that more organisations are opening parts of their systems to employees, customers and other businesses via the Internet [37].

In this study, it is also important to delineate the scope of information security in relation to other similar concepts such as information assurance and defensive information warfare. Like defensive information warfare, both information security and information assurance address intentional threats. Information Security has often been decomposed into the "CIA" model of information security whose components are confidentiality, integrity and availability. The study uses the CIA model of information security and defines information security as the organizational processes, policies, procedures, and systems implemented by an organization in an attempt to prevent the unauthorized intentional or unintentional reduction of the confidentiality, integrity, and availability of proprietary or sensitive organizational information, whether in storage, processing, or transit [3].

2.3 Definition of Insider Threats

CERT have defined the term "insider" as "individuals who were, or previously had been, authorized to use the information systems they eventually employed to perpetrate harm [9] "the term insider threat refers to threats originating from people who have been given access rights to an and misuse their privileges, thus violating the information security policy of the organization. Based on these prior definitions, it is our view that the insider threat refers to both intentional and unintentional violations, of organizational security policy.

For the purposes of this study, we adopt the definition of the insider threat by CERT. , the definition indicates that the organizational security policy delineates how individuals within the organization use, protect, and control organizational information, the systems used to process it, and any intentional deviation from the policy is considered an information security violation[7], [9]. Both intentional and unintentional violations of the organizational security policy can pose a significant threat to organizational security [7].

2.4 The Drivers of Insider Threats

Sabotage is often caused by employees who become disillusioned with their company, boss, or co-workers, including displeasure with compensation, reprimands, and job termination [7], [14]. Additionally, hostility can arise when employees feel underappreciated, stressed, overworked, unfairly treated and or isolated such that they exert their anger or revenge by performing an inside attack[12]. Sabotage is usually executed by employees with high technical skills and access to critical assets, such as ICT engineers and System Administrators who have the ability to cause implausible damage [14]. During the study, it was discovered that most ICT departments are understaffed, and are likely to suffer stress due to work overload [3], [4], [15]. This could trigger an insider to commit a crime against the organisation. Hence the reason to undertake this research. Some of the recorded means for misuse of organisational information by potential insiders include but not limited to printing, emails, copiers, web posts, blogs, and social media chats etc. [12].

CERT states that non-malicious insiders cause ICT security incidents accidentally for different reasons that include; human error, lack of user awareness, drugs, fatigue, stress, moods, gender issues, drugs, age and or cultures. These accidental threats are referred to as "Unintentional Insider Threat (UIT)" the most common examples includes security incidents, which insiders can cause such as excessive access rights being granted to wrong users, introducing vulnerabilities during software development when SDLC steps are bypassed, leaving an unencrypted portable storage device unattended to, system configuration errors, inactivating security controls [7].

2.5 The Indicators that Review that Insiders are at Work

An insider threat can be present or develop over a period of time with indications that an organisation can categorize as "direct" or "indirect", with each requiring different types of tracking mechanisms. The direct risk indicators are usually anomalous activities that deviate from normal day to day work activities, such as accessing sensitive information that bears no direct relevance to normal job duties, downloading large volumes of data to external drives, or even emailing confidential data to a personal account. On the other hand, the Indirect risk indicators are usually patterns of human behaviour that require analysis to reveal suspicious motives such as expressing the desire to resign over social media, sudden overuse of negative emotive words in communications and demonstrating ties to high-risk personnel[38].

Apart from the indirect and direct indicators discussed above, other common insider threat indicators include [39];

i. Attempts to evade defined security controls and policies
ii. Requests for higher-level access privileges without a convincing reason
iii. Frequent access to workspace outside normal working hours
iv. Irresponsible social media habits
v. Maintaining access rights to sensitive data after job termination
vi. Visible disgruntlement toward employer or co-workers
vii. The decline in work performance
viii. Behaviours that demonstrate sudden affluence without obvious cause, such as large pay raise, inheritance, etc.
ix. Remotely accesses the network while on vacation, sick or at odd times
x. Works odd hours without authorization
xi. Notable enthusiasm for overtime, weekend or unusual work schedules
xii. Unnecessarily copies material, especially if it is proprietary or classified
xiii. Interest in matters outside of the scope of their duties

All these red flags must not be viewed as demonstrations of harm, but they should rather invoke a process for review and clarification. The review process needs to integrate the risk indicators as well as analysing them collectively so as to uncover hidden relationships. This usually reveals more detail than when they are examined individually. To assess these risk indicators, organisations need to access both structured and unstructured data sources. Some examples of data and risk pairs include [38], [39];

i. Travel and entertainment data, a violation of corporate policies
ii. Network access data - web browsing history, network crawling, data hoarding, copying from internal repositories
iii. Physical facility access logs - anomalies in employee work hours, attempts to access restricted areas
iv. Travel records - countries known for IP theft or hosting competitors
v. Phone logs - calls with known high-risk personnel or external parties
vi. Emails/instant messages - malicious intent
vii. Human Resources (HR) records - terminations, layoffs and performance issues
viii. Employee hotline logs - complaints of hostile, abnormal, unethical or illegal behaviours
ix. Operating System – High amount of data transferred from endpoint to Universal Serial Bus (USB) or Compact Disc (CD) / Digital Versatile Disc (DVD)

x. File Server / Database – Abnormally high number of files downloaded to some location.
xi. Email Server / Web Proxy – Abnormally large amount of data emailed or uploaded to the file-sharing site (i.e. DropBox)
xii. Web Proxy – User browsing websites on a watch list (i.e., competitors, job sites)
xiii. Physical Access Control System – Unusual physical access attempts (i.e., after hours, secure areas without authorization)
xiv. Printer Logs – Employee on a watch list due to demotion, poor review, or impending layoff
xv. Human Resources (HR) Systems – Employee on a watch list due to demotion, poor review, or impending layoff
xvi. Active Directory / HR Systems – Username of a terminated employee accessing internal systems
xvii. Operating System / Active Directory – IT Admin performing an excessive number of deletions on critical servers or password resets.

Signs of vulnerability, such as drug or alcohol abuse, financial difficulties, gambling, illegal activities, poor mental health or hostile behaviour, should trigger concern. Be on the lookout for warning signs among employees such as the acquisition of unexpected wealth, unusual foreign travel, irregular work hours or unexpected absences [39].

2.6 Insider Threats Detection, Prevention and Response

Detecting and preventing insider threats is a difficult task, but if organisations are able to identify the most critical assets and ensure that they have good visibility into the activities of those assets, the chances for detecting unauthorized activities increases and significantly reduces the likelihood that an insider will be able to execute a successful attack[40]. Organisations must stay vigilant against external threats, but should not ignore the risk that insider threats pose to sensitive data. Insider threats pose a significant risk to organisations such that any accidental or malicious act by an employee can potentially lead to catastrophic incidents that threaten the corporations' reputation. However, despite the risks insiders pose, organisations are still required to give employees access to company data in order for them to perform necessary job functions. Despite the fact that it is difficult to implement controls that are able to detect or mitigate these risks, there are processes that organisations can develop to reduce the chances of an insider threat being successful [37], [40].

2.6.1 Detection

Much as it is difficult to detect insider threats, there are some processes that public organisations can develop or enhance to increase their possibilities of detecting insider threat activity such as[40],[41];

i. Identifying critical data assets and baseline employee data access activities to increase the chance that anomalous insider behaviour can be quickly identified
ii. Enforcing mandatory vacations and job rotations so that employees remain fresh and alert, thus increasing the likelihood that malicious insider activities are detected; It may be surprising that a large number of dark-side insider threats are noticed when people take a vacation
iii. Periodically rotate responsibilities for sensitive functions
iv. Separate responsibility for detection setup and detection monitoring dual controls
v. Separate responsibility for sensitive operational functions
vi. Ensure that data protection mechanisms are established and will alert for unauthorized data transfers such as sensitive data sent via email, data copied to removable drives
vii. Conduct regular security awareness training that stresses the importance of identifying and reporting insider threat activity to the appropriate security teams, phishing/spear phishing, and spam
viii. Monitor for unusual outbound traffic patterns, including such as Odd connections to unknown IP addresses, Unusual connection length times for outbound connections and an abnormally large amount of data transferred from the environment
ix. Data / file encryption
x. Data access monitoring and control
xi. Intrusion Detection / Prevention Systems (IDS/IPS)
xii. Data Loss Prevention (DLP)
xiii. Enterprise digital rights management and
xiv. Data redaction
xv. Elements of an Effective Response to an Insider Attack..

2.6.2 Prevention

Insider threats prevention is just as perplexing as detecting insider activities since employees have approved access to company information assets. However, there are still some processes that

public organisations can implement to reduce the chance of an insider compromising the integrity, availability or confidentiality of organisational data. Among them, a few are as listed [40];

i. Develop security enclaves like network segmentation and segregation where sensitive company data is housed
ii. Implement processes to detect unauthorized attempts to transfer data from these enclaves
iii. Follow the principle of "role-based" and "least privilege," for access control
iv. Implement preventative controls such as USB and internet port security
v. Implement data loss prevention (DLP) technology that can be used to analyse company emails and reduce the chance that an insider can email sensitive data from the environment
vi. Monitor egress traffic and detect unauthorized uses of encryption, which may indicate an attempt to remove data from the environment
vii. Provide regular security awareness training and stress that employees should validate emails prior to opening attachments and click on links.

2.6.3 Response

To respond to an insider attack, organisations should [40], [41];

i. Ensure your Incident Response Plan (IRP) has provisions for Insider Threats
ii. Have a process to investigate and document incidents
iii. Be committed to responding based on evidence so as not to end up accusing a dedicated and trusted employee that is doing good work
iv. Use detective controls and digital forensics to back up the claim
v. Be prepared to act quickly
vi. Be prepared to restore because a disgruntled employee may just want to do damage.

It's also important to keep in mind that in the case of insider threats, a Cyber Security culture can be one of the best deterrents for both the malicious and the accidental. Because how an organisation is managed can discourage insiders from even trying [42].

2.7 The Consequences of Insider Attacks

2.7.1 Loss of Value

Insider threats can also have a direct impact on all the three categories of values in a business venture namely; intrinsic value, market value and revenue which refers to the monetary qualities of the business. The Market and intrinsic value of a business since intellectual property comprise 50 to 80% of the businesses value [42]. Theft of new product designs and strategies can have catastrophic consequences. Revenue can also be impacted directly by insider events. The intellectual property theft at American Superconductor immediately resulted in the loss of $800 million in revenue. According to Cisco, nearly one-third of businesses that suffered a breach lost more than 20% of their revenue [38], [42].

2.7.2 Operational Disruption

Operations refer to the ability of a business to execute its mission. There three general categories of operational impact include operational disruption, increased overhead, and remediation costs. Operational disruption is usually difficult to quantify but includes unplanned expenses, increased staffing and inability to deliver goods and services. A detailed study by Deloitte estimated that for a large company that suffered intellectual property theft, the five-year operational disruption cost would be a whopping $1.2 billion [38].

2.7.3 Increased Overhead

Increased overhead due to necessary Cyber Security improvements, staff retraining, etc. also impact business operations and can exceed $13 million for a large corporation [39].

2.7.4 Remediation Costs

According to the Ponemon Institute, the average remediation costs was $4.3 million in 2016 but decreased to $3.6 million in 2017. However, according to Deloitte, the remediation costs can be much higher and exceed over $10 million. This is, of course, largely fact-specific depending on the size of the organization, the degree to which the organization was harmed, and the required mitigation actions needed [39], [42].

2.7.5 Reputation

Reputation impact can be assessed by examining three areas: public relations expenditures, customer relationships, and the devaluation of trade names. Reputation, although difficult to quantify, is often the second most affected aspect of the business following a compromise – second only to value. According to Cisco, half of the organisations that were breached expended significant resources to actively manage the reputation and 42% of them lost nearly 20% of their existing customer base. Moreover, a detailed study by Deloitte uncovered that new customer acquisition decreased by as much as 50%. The study also revealed that large companies spent an average of $1,000,000 during a 12 month period to restore their reputation. The same study revealed a large company could experience an impact of $250 million over a five-year period by the devaluation of its trade name alone [38], [39], [42].

2.7.6 Culture

Culture is often ignored when impacts are discussed, however, culture is the lifeblood of any organization. Culture holds the shared values, norms, beliefs and assumptions that ultimately drive employees' actions. According to the Society for Human Resource Management, typical businesses experience 24% turnover each year and most employees only stay 4.5 years in a position millennial stay even less at two years on average [38]. This results in financial and logistical problems, but also data protection problems. According to research, most employees intentionally take confidential data with them when they leave and most will seek to use this to the detriment of the organization. Add a significant corporate impact such as a data breach to this equation and the impact on culture is dramatically magnified. This can result in an additional turnover, increased distrust, and an eroding of morale all which can exacerbate the effects of a breach. In short, culture shapes everyday behaviour and a bad culture will lead to bad behaviour [39], [42].

2.7.7 Liability

Liability refers to the external costs that are levied on an organization. Liability costs include compliance fines, breach notification costs, increased insurance costs, and litigation costs including attorney fees. These costs can be large ranging from $20 per record per customer breach to $3 million in litigation costs, a 200% increase in insurance costs, and fines that can exceed $1 million. Moreover, litigation settlements can exceed tens of millions of dollars for large breaches [39], [42].

2.8 Factors Leading to Insider Threats in Public Organisations

The Computer Emergency Response Team (CERT) states that insiders cause ICT security incidents accidentally for different reasons that include; human error, lack of user awareness, drugs, fatigue, stress, moods, gender issues, drugs, age and or cultures. These accidental threats are referred to as "Unintentional Insider Threat (UIT)" the most common examples includes security incidents such as excessive access rights being granted to wrong users, introducing vulnerabilities during software development when Systems Development Life Cycle (SDLC) steps are bypassed, leaving an unencrypted portable storage device unattended to, system configuration errors, inactivating security controls, voluntary rule breaking, self-benefiting without malicious intent [15]. These are insiders who can cause damage to an organisations resources through their actions unintentionally. Insiders both malicious and non-malicious can motivate the success of these non-targeted malware exploits in various ways that include, exposing the organisation in social engineering attacks, being a doorway of malware onto the network by using infected removable storage media, opening unsafe attachments and or visiting hostile websites [9]. They are capable of incidentally putting the organisational information at risk due to the fact that the accepted work processes they operate, are risky or simply because there are neither right tools in place nor the right awareness training provided. For instance, it may be a common practice that employees put alternative email addresses on their business cards and also carbon copy their work to themselves on these consumer-grade web-based email systems including Yahoo, Icloud, Hotmail or Gmail. They can also share documents with others using personal storage solutions like Google Drive, Evernote, Icloud, Dropbox. These personal Internet hosted systems take the organisational resources beyond the system of control which can put it at risk of compromise [9]. Among other factors includes; difficulty in modelling human behaviour, lack enterprise risk management, the complexity of the insider problem, lack of viable insider mitigation strategies, lack of Information Classification, access-control failure, misuse and defence by-pass and lack of user awareness on access, management hygiene and establish business rules of information management.

Difficulty in Modelling Human Behaviour: Insider threat is not one problem, but various because modelling human behaviour is close to impossible which is a recorded limitation. Most perpetrators commit the crime while on duty having planned their actions so well, due to financial gain and the sophistication of technology [15].

Lack Enterprise Risk Management: Most public organisations lack enterprise risk management, therefore, there is need to identify physical locations of critical data assets, advocate for user awareness on access management, adopt a risk-based approach and establish business rules of information management. Public organisations need to consider legal and regulatory implications in insider mitigation as well as adopting a risk-based approach [38]. Most incidents require little technical and sophistication because insider perpetrators plan their actions before effecting an attack, with a motivation of financial gain. Reducing the risk of these attacks requires organisations to look beyond their information technology and security to their overall business processes [4].

The Complexity of the Insider Problem: Intruders into information systems are either employees or others who are internal to the organization. Insider threat mitigation is a complex problem and research is in its infancy, therefore, there are opportunities for further research in this area. There is a need to develop granular attack trees for the rich variety of insider threats [44]. It is common knowledge that most public organizational shareholders are more sympathetic to organisations who have security breaches caused by externals than internals [44]. This highlights the need for research on the complexity of the insider problems, which are a factor leading to organisational insider threats because all employees need access to the relevant systems for them to be able to carry out their day to day tasks.

Lack of Viable Insider Mitigation Strategies: Most Parastatals security controls have no viable insider mitigation strategies with no pointer to the extent of security and controls needed to be implemented. There is a need for them to customize their mitigation strategies according to the organizational goals so as to enable a multi-tiered insider threat plan of action as well as tailoring countermeasures and policies to meet continuous monitoring and identify abnormal behaviour and usage patterns [45].

Lack of User Awareness of Access, Management Hygiene and Establish Business Rules of Information Management: There is a positive linear relationship between organisational Cyber Security Preparedness and employee attitudes to security policies adherence. Therefore, implementing Cyber Security programs in Zambia's public organisations cannot be successful without careful consideration of the legal and regulatory implications. There is a need to adopt a risk-based approach, identify physical locations of their critical data assets, advocate for user awareness of access, management hygiene and establish business rules of information management [32]. Public organisations should carry out Vulnerabilities Assessments (VAs)

targeting the security strategies and controls applied to protect the systems from insider attackers [32].

Organisations should alleviate users' limitation of knowledge in the organization's policies and procedures by conducting awareness training. Insider threats mitigation depends a great deal on the researcher's experience, knowledge and network [46].

Lack of Information Classification: There is a need for improvements in information and assets classification, accompanying policies and ICT risk assessment. Most information security process is not embedded in public organisations operations, therefore, there is no insight into the actual threats to information security [24]. Awareness and business Policies should be established as well as the security maturity level of all organisations [47].

Access-control failure, misuse and defence by-pass: insiders should not have access to specified resources. This is a technical problem and, while prevention is straightforward, detection of access-control failures is difficult same as with access-control misuse [4], [41]. Access misuse - the insider has rights and within those rights can misuse system resources, probably the hardest form of attack to detect or prevent technically, since the insider already has legitimate access [4],[32]. Defence by-pass - insiders already inside the perimeter, and therefore have more opportunity for mischief. Purely technical defences are insufficient because if they worked, the problem would not exist. Dependence on technical or non-technical detection of anomalous behaviour or actual attacks is vital [4], [32].

2.9 Insider Landscape

In the recent past, organisational insider attacks have grown exponentially. Take for instance, in 2007, a study by KPMG reviewed that only 4% of the total recorded cyber incidents were instigated by malicious insiders [26]. Three years later the figure increased to 20% and 2013, Verizon's extensive review stated that 69% of information security incidents were ascribed to insider threats [16]. The growing dimension of threats to insider can be evidenced by the revolution of the internet and the growth of the Internet of things (IoT). However, knowing what exactly motivates inside threats is the right path to finding a strategic solution of how to mitigate the problem to an acceptable level [16]. Table 2.1 gives a highlight of insider case progression as researched by various reputable organisations from 2000 to 2017.

Table 2.1: Insider threat progression

No.	Author	Survey / Study	Organisation	Insider threats
1.	KPMG – 2007	The threat from within [26]	KPMG	4%
2.	KPMG – 2017	The threat from within [26],[28]	KPMG	20%
3.	Christopher King - 2012	Malicious insiders and organized crime activity [21], [23]	CERT	16%
4.	Verizon Risk Team – 2013	Data breach investigation [16]	Verizon	69%
5.	Digital Guadian – 2013	Insiders Vs. outsiders what's greater Cyber Security threat infographic [22]	Digital Guadian	59%
6.	Vormetric – 2015	Insider threat report [19]	Vormetric	83%
7.	Avecto – 2016	Mitigating risk by removing user privileges [27]	Microsoft	94%
8.	T. McDaniel, et al - 2016	Security Survey [18]	Forrester's Global	77%
9.	M. Spilter, et al – 2017	Data breach investigation [16]	Verizon	78%

2.10 Recorded Insider Incidences

Management and Education of the Risk of Insider Threat (MERIT) and Defence Personal Security Research Centre (DPSRC) records various insider attack vectors' incidences in their database of insider incidents maintained with related research conducted by CERT which has numerous entries from public sources, collected since 2001 for misuse of organizational information by potential insiders includes but not limited to printing, emails, copiers, web posts, blogs, and social media chats and many more as shown in Table 2.2.

Table 2.2: Insider recorded incidences.

No.	Incidence	Agent	Details
1.	Banking sector	Branch manager	A case of a manager for a branch of a banking institution who stole over $225,000 from the business account after running into family health problems, gambling and unforeseen expenses [23], [26].
2.	POS System	Secretary	In a case of a secretary who worked at a youth organization for over 20 years, used a point-of-sale system to issue at least 500 fraudulent refunds totalling over $300,000 to the insider's own bank account over a 5-year period [23].
3.	Cell Phone Clones	Group of insiders	In a case of a group of insiders at a wireless telecommunications company who cloned more than 16,000 customer cell phones. The insiders made approximately $15 million worth of unauthorized calls for a period of six months [23].
4.	Copier	Army signals analyst for NSA	A case of Sheldon Boon, an Army signals analyst for NSA, who used a handheld scanner to copy 52 classified documents and later passed to the Soviets[23], [25].
5.	Email	FBI intelligence analyst	A naturalized U.S. citizen from the Philippines while working at the FBI as an Intelligence analyst, took and transferred classified information to senior political officials of Philippines in an attempt to overthrow that country's government [23], [25].
6.	Printing	Department of Navy (DON) computer specialist	A case of Robert Chaegun Kim, a South Korean born American computer specialist working for the Department of Navy (DON) at the Office of Naval Intelligence. He used his insider access to find classified documents, delete the classification markings and printed them out to mail to his South Korean contacts [23], [23].
7.	Classified information Leakage	intelligence analyst	WikiLeaks: A case of Bradley Manning, an American Army soldier who in his role as intelligence analyst, leaked the largest set of classified documents to the public as he worked as an intelligence analyst [22].
8.	SCADA	Electrical supervisor	In a case of an electrical supervisor who developed an application for a SCADA system which was being used by the water firm. He installed a malicious program on one of the organization's critical systems, after his contract termination and damaged the SCADA system [23].
9	Social Media posting incidence	University of Professor	In a case of a University of Tennessee professor who relayed sensitive data to China, while he emailed the other classified documents to his private email address. [23].

2.11 Related Works

Table 2.3 highlights various related works in mitigating insider related threats and risks that were reviewed for the fruition of this research

Table 2.3: Related works.

No	Title	Author	Key Findings	Limitations/ Gaps
1.	Mitigating malicious insider cyber threat[44]	Jason Anthony Smith – 2015 UK.	• 87% percent of identified intruders into information systems are either employees or others internal to the organization. • Insider threat mitigation is a complex problem	Development of granular attack trees for the rich variety of insider threats • Public organisational shareholders are more sympathetic to organisations whom have security breaches caused by externals than internals
2.	A Framework for Assessing the Insider Threat in Parastatals [45]	Michael Juma Abuli – 2016 Kenya	• Kenyan parastatals controls and countermeasures has no viable insider mitigation strategies • There was no pointer to the extent of security and controls needed to be implemented at these layers.	• Parastatals customization of insider threat plan of action and mitigation strategies to align to corporate goals • Tailoring public organisation's countermeasures and policies to meet continuous monitoring, to identify abnormal behavior and usage patterns (awareness)
3.	Managing insider threat [38]	Jim McCurry et al – 2016, USA	Public Organisations need to: • Identify physical locations of their critical data assets • Advocate for user awareness on access management	• Consideration of the legal and regulatory implications of insider mitigation. • Adopt a risk-based approach
4.	Investigating Insider[47]	W.Cornelissen – 2009 Finland	• Need for improvements in information classification, related policies and ICT risk assessment	• Adopting a risk-based approach and critical assets classification • Awareness and established business Policies • Security maturity level of firms.
5.	Norwegian Approach in- Insider Threat [46]	Terje Benjaminsen, 2017 Norway	• 76% cases are self-initiated (insiders) • Motivation -financial gain 47%, ideology 20%, desire for recognition 14%, loyalty 14%, and revenge (6%).	• Users limitation of knowledge in an organization's policies and procedures • Qualitative research depends a great deal on the researcher's experience, knowledge and network

No	Title	Author	Key Findings	Limitations/ Gaps
6.	Factors determining Zambia's Cyber Security preparedness [32]	Collins C. Kachaka , – 2016 Zambia	• Banks' preparedness to fight cybercrime varied from neutral to agree • There is a positive linear relationship between Banks' Cyber Security Preparedness (BCP) and bank staff attitudes & security policies	• Larger scale investigation targeting the examination of security vulnerabilities • Strategies applied for and factors contributing to insider hacking of bank systems • The extent of ignorance contribution towards perpetration of cybercrimes
7	Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector[43]	Marisa Reddy Randazzo et al – 2005 USA	• Most insider attack incidences require little technical sophistication • Insider attack perpetrators plan their actions in advance before attacking • Most perpetrators are motivated by financial gain and the sophistication of technology • Victim organisations suffered financially	• Reducing the risk of these attacks requires organisations to look beyond their information technology and security to their overall business processes • Most organisations executive management have continued to keep a blind eye to warnings concerning insider threats due to the high cost of implementing improved security
8.	Insider Threats An Overview of Definitions and Mitigation Techniques [15]	J.H. Associates LLC & Christian W. Probst, - 2008 Denmark	• Most incidents required little technical and sophistication, insider perpetrators planned their actions before attacking as motivated by financially gain and that most victim organisations suffered financial from insider perpetrators.	• The researcher further recommended that reducing the risk of these attacks requires organisations to look beyond their information technology and security to their overall business processes
9	Detecting Malicious Insider Threat in Cloud Computing Environments by Thesis Piraeus[8]	Nikolaos Pitropakis – 2015 Greece	• Identified that malicious insider threat as one of the major ones, without sufficient countermeasures • There are malicious insiders that was introduced along with the cloud computing, which has multiple roles and more attack points than an outsider	• There is a need to investigate the cloud infrastructure in depth in order to check whether a potential attack can be detected • There is need to focus on adding extra layers of either cryptography or steganography to the authenticator, in order to increase the security level without significantly increasing the overhead introduced

No	Title	Author	Key Findings	Limitations/ Gaps
10.	Analysis of Insiders Attack Mitigation Strategies	Zulkefli Mohd Yusopa and Jemal Abawajy - 2014 Australia	• The steps of embracing Cloud storage service has led to security problems • An attacker that has access to the cloud storage component is able to take snapshots or alter data in the storage. • One of the most serious challenges, not only in cloud computing but to data security in general, is the insider threat	• Once data is in the cloud and users no longer physically possess their data, its confidentiality and integrity can be at risk • The main security concerns of clients are a loss of direct control of their data and being forced to trust a third party provider with confidential information. • A malicious insider, such as a cloud administrator, can easily inspect the virtual machines of cloud users and retrieve sensitive information

2.12 Insider Threat Attack Vectors

2.12.1 Access Control Attack Vector

The ideal access-control policy simultaneously grants the user sufficient privileges to perform necessary tasks, while constraining access according to a set of rules. The rules are based on principles of least privilege, escalation and separation of duties [4],[40]. Access control is the mechanism of providing and limiting access to electronic resources based on a set of credentials. The two components of this mechanism namely, authentication: showing who or what you are, by demonstrating possession of certain credentials and authorization: determining if your credentials are sufficient to provide you with a requested type of access. The extent to which explicit, fine-grained access controls can be defined and enforced shapes very directly the type of insider misuse that might occur [4],[41].

In its basic form access control maps users with access to resources. Role-Based Access Control (RBAC) is a finer-grained method that maps defined roles with access to resources. Temporal RBAC extends this method by specifying time constraints on when a role can be enabled or disabled. Different methods of implementing access control have also been proposed, more importantly, that access control policies also need to be able to specify monitoring and auditing requirements [4]. However, access control has a number of limitations, because even perfect access control will not prevent insider attacks who are only using privileges that are deemed

necessary for their daily task. Various studies show a disconnect between what real-world practitioners desire and what the research communities offer. Meanwhile, limiting access legitimately can have a negative impact on the productivity for non-malicious employee [4],[40].

2.12.2 Cloud Attack Vector

An analysis of insider attacks mitigation strategies by Zulkefli M. Yusopa and Jemal Abawajy reviewed that anyone with access to the cloud storage component is able to take snapshots or alter data in the storage. Security is the biggest issues in Cloud Computing as it offering storage service at a remote location that the consumers generally need to trust the Cloud provider and unaware of what happens to their data [48]. Therefore, insider security is one of the biggest issues in cloud computing as it offers storage services on a remote location that the consumers generally only need to trust the cloud provider and are unaware of what happens to their data. Among security threats in the cloud, malicious insider threats pose a serious risk to clients [48]. Once users no longer physically possess their data, its confidentiality and integrity can be at risk. The main security concerns of clients are a loss of direct control of their data and being forced to trust a third party provider as in Fig 2.1 with confidential information. Among security threats in the cloud, insider threats such as malicious system administrators pose a serious risk to clients [49].

Fig 2.1: Cloud Storage [49]

Data that is resident in Cloud Systems suffers the risk of Confidentiality, Integrity & Availability. The issues of keeping information secure and confidential in a cloud storage system are paramount. The owners of the cloud service system have literal control over the data they hold on behalf of their customers and this may imply that they can modify data to their liking without the data owner's consent. This act amounts to insider threats. Cloud systems are internet based making

them accessible to both insiders and external hackers [49]. The difficulty, therefore, is managing access control.

2.12.3 Data at Rest Attack Vector

Data-at-Rest Risk Factors: The identified risk factors targeted at secondary storage medium includes; Media Theft- where the device containing the data gets stolen [4],[50]. Data Corruption where the data held on the device or flash-drive gets corrupted due to incorrect usage [4]. Storage Wear (flash-drive) refers to the wear and tear of the storage device due to time or age. A flash drive memory cell's lifetime is finite and each flash drive memory cell has limited endurance. The data written and deleted onto or from the device cannot be done time beyond a certain number (reprogrammed continuously). Each flash drive memory cell is called a Single Level Flash Cell (SLC) and each SLC has an industrial tolerance of approximately 10k Program/Erase (P/E) cycles while a 2-bit Multi-Level Cell (MLC) has an industrial tolerance of about 3k P/E cycles. Data Diddling - A possibility exists where an attacker can fiddle with the data held on the storage device (flash drive) before handing it over to systems users for either storage or processing [4], [51].

2.12.4 Biometrics Attack Vector

We discuss the potential privacy pitfalls arising when using a biometric identifier. Biometric can expose sensitive data such as information about one's health and the racial origin and this information can then provide a basis for unjustified discrimination of the individual data subjects [50]. The possible attack vectors in biometric systems have been showcased from different viewpoints. The first being the scheme of Fig 2.2, by the international standard ISO /IEC JTC1 SC37 SD11. This identifies where possible attacks can be conducted as in Figs 2.3 and 2.4 [4].

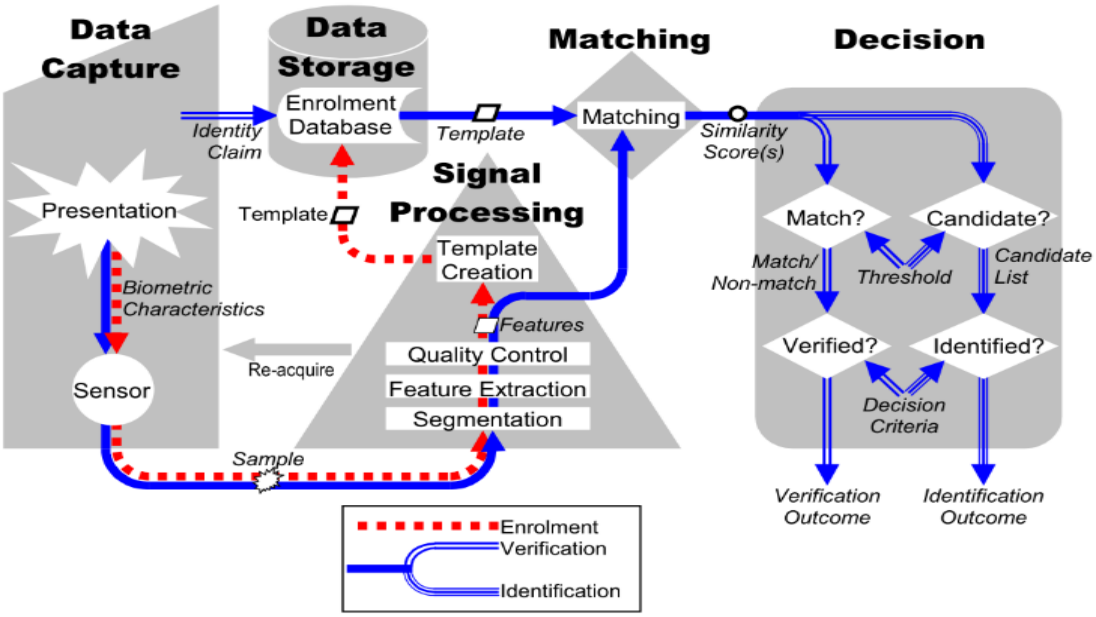


Fig 2.2 : ISO Illustrations of error rates for different biometric modalities [4]

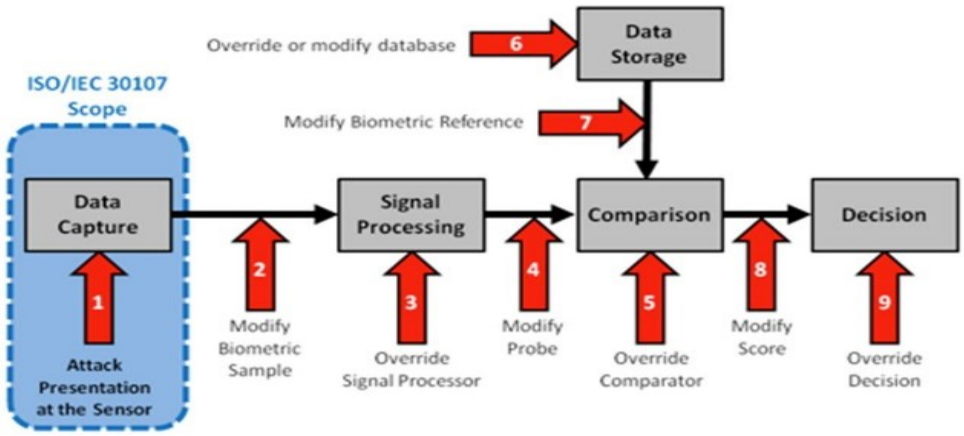


Fig 2.3: ISO's model attack framework [4]

All biometric systems involve two steps namely Enrollment step and a verification step. ISO 30107 illustrates a presentation of a biometric attack detection [4].

International Business Machines (IBM) researchers identified and categorized a number of the biometrics related attacks. These attacks are intended to either circumvent the security afforded by the system or to deter the normal functioning of the system as in Fig 2.4;

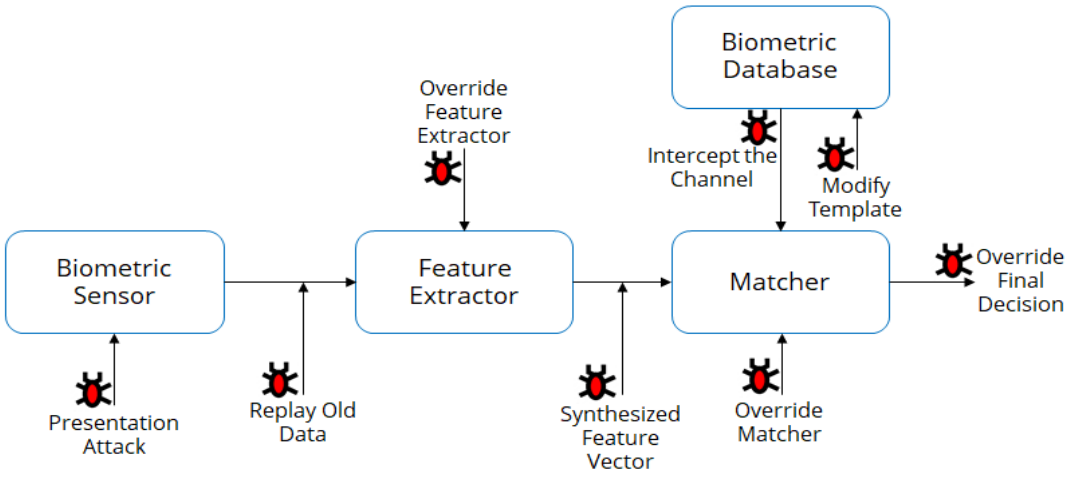


Fig 2.4: IBM's biometric threat model [4]

Presentation Attack – Spoofing the biometric trait, such as with a finger mould, presented at the sensor, Replay Old Data – Resubmitting illegally intercepted data to the system. Override Feature Extractor – Overriding the feature extractor to produce predetermined feature sets. Synthesized Feature Vector – Replacing legitimate feature sets with synthetic feature sets. Override Matcher – Overriding the matcher to output high scores, thereby defying the system security. Modify Template – Compromising the templates stored in the database. Alternately, introducing new templates to the database. Intercept the Channel – Altering the data in the communication channel between various modules of the system. Override Final Decision – Overriding the final decision output by the biometric system. Several security techniques exist to thwart attacks at various points, including encrypting communication channels, using mutual authentication, placing the feature extractor and the matcher in secure locations, and limiting unsuccessful attempts[4], [44].

2.13 Insider Threat Mitigation Models and Programs

2.13.1 Model

Insider attacks landscape has shown an exponential growth in the recent past. This can be evidenced by a number of research that has been done globally by both academics and big business players such as CERT, SysAdmin, Audit, Network, and Security (SANS), IBM, KPMG, Verizon, PricewaterhouseCoopers (PwC), Ernest and Young (EY), Deloitte and Touche, Microsoft as well as the uprising of the of Internet of things[7],[13],[16],[28],[29]. The challenge necessitates an understanding of ANT in order to have knowledge of the link between human and circumstantial factors that include; technological, sociological and social-technical domains in which the insiders

operate. This is because technology alone has the potential of enhancing the challenge than otherwise. The predicament has led many researchers to endeavour in studying TPB and individual behaviour, with an aim of mitigating insider threats. Despite all the global efforts and the results, no such research efforts have been employed in Zambia to address Insider threats mitigation [32].

Recent surveys by Forrester's Global Business Technographics showed that internal fraud risks are an area that has long been managed using forensic data analytics and ranked as the top use case at 77%. While Cyber breach and sabotage ranked the second-highest risk area at 70% [18], [29]. It is, therefore, imperative that internal attackers, generally accounts for approximately more than half of the risks that an organization is exposed to, whilst the external threats account for approximately above a third of the risks despite the gravity of the external consequences to an organization [19].

2.13.2 Insider Threat Programs

A number of a reputable organisation such as CERT, ISO 27001 among others have considered adopting programs to mitigate Insider threats as in Figs 2.5 and 2.6. These are step by step elements that are required by an organisation that is cyber security conscious and endeavours to be cyber ready in mitigating insider threats. However, they fail to implement due to high cost of implementation and continuous improvement processes. In the direction of adopting industry best practices for the stated solution and strengthening the insider threat mitigation program, we decided to adopt some components from the CERT's Insider Threat program as shown in Fig 2.5 and ISO 27001 model in Fig 2.6 such as adoption of security policies, security procedures, training and awareness, compliance, Human resource security, supplier security, integration of Enterprise Risk Management and Incidence response or management among others that are necessary to produce a fully functioning insider threat program to suit Zambian public sector [7], [17].

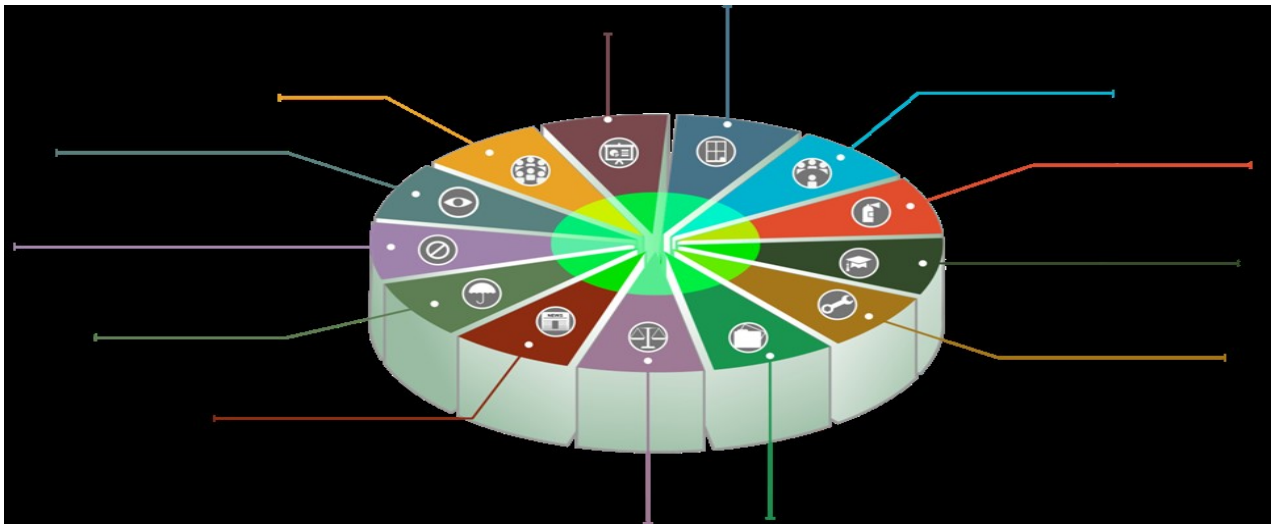


Fig 2.5: CERT Insider Threat Components[7].

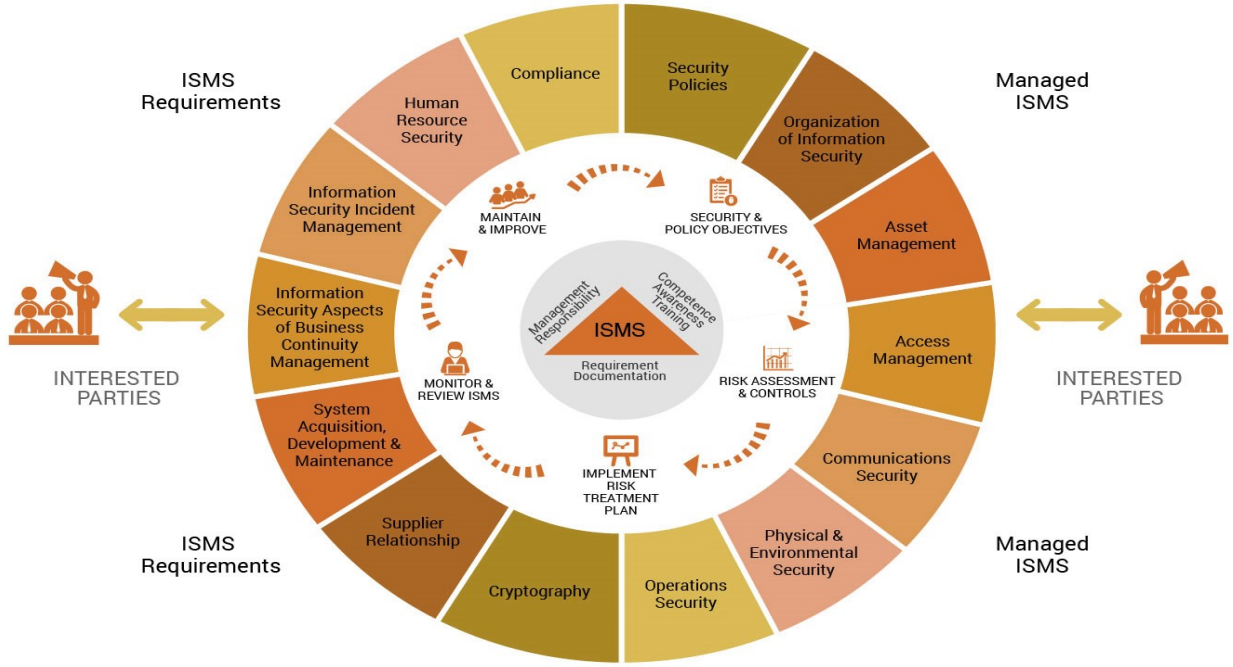


Fig 2.6: ISO 27001: ISMS Requirements[17]

Ernest and Young's (EY) Insider Threat Program Framework which leverages the work of the United States of America (USA) and United Kingdom (UK) CERT, the Intelligence and National Security Alliance, the National Institute of Standards and Technology, and the Centre for the Protection of National Infrastructure, helps organisations develop an integrated risk management program to protect their critical assets against insider threats [38]. It offers a data-driven approach to manage insider threat risk while taking advantage of the advanced analytical tools and information governance disciplines. This was created with the assumption that the insider threat program should be fully integrated with the organization's existing corporate security and Cyber

Security programs. Insider threat needs to be part of enterprise-wide risk management considerations, aligned with organizational risk priorities. An insider threat program is far more than a technical program. Given the nature of insider threats, the human element is just as important as the technology. The human consideration needs to be embedded in every aspect of the insider threat program, from policymaking, monitoring and escalation procedures to consequence management [38],[39].

2.14 Chapter Summary

This chapter discussed the literature and the related studies which met its objectives by comparing and contrasting the previous works of other researchers and provide support for the development of a proposed Insider cyber threat mitigation model to reduce the risks associated with insider threats to an acceptable level. It discussed a number of factors affecting insider security management in public organisations. It highlighted the meaning of ICT/Cyber Security culture in organisations, the various indicators to ICT/Cyber Security and how they can be related to the public organisations. Numerous challenges were identified from the various literature reviewed. The ultimate conclusion of the chapter from the literature reviewed indicated the gaps in the factors and challenges to organisational ICT/Cyber Security culture.

CHAPTER THREE

RESEARCH METHODOLOGY

3.1 Introduction

In the previous chapter, literature was reviewed with an aim of establishing the challenges encountered by the other countries' Public Organisations in mitigating insider threats and identifying factors leading to the insider attacks and or information leakage in Zambia. A critical analysis of how insider attacks impact on the productivity of the nation through the public organisations was considered. Having laid the basis for the study, this chapter discusses the approach taken in the collection and interpretation of research data. It entails formulating the problem to investigate, selection of the suitable research design, procedures for data collection, the target population and the sampling technique, that was used. It will also cover the research instruments, the data analysis technique as well as the ethical considerations.

Research methodology denotes an approach and procedure of a logical process which is applied to a scientific investigation. This approach concerns an available technique for data collection, coding, entry, processing and analysis [52]. Consequently, the proposed philosophy adopted by this research was positivism perception which proposes scientific methods as a means of knowledge generation and that the data collection techniques to use include small samples and quantitative in nature [53].

This methodology is as illustrated in the process flow diagram in Fig 3.1 in that order. The research problem is encapsulated in the research objectives below.

The objectives of the study included the following:

i. To establish the types of vulnerabilities in public organisations that can be exploited by insiders
ii. To establish the effectiveness of the current controls in public organisations in protecting against potential Cyber Security threats from insiders
iii. To propose measures to mitigate insider threats.

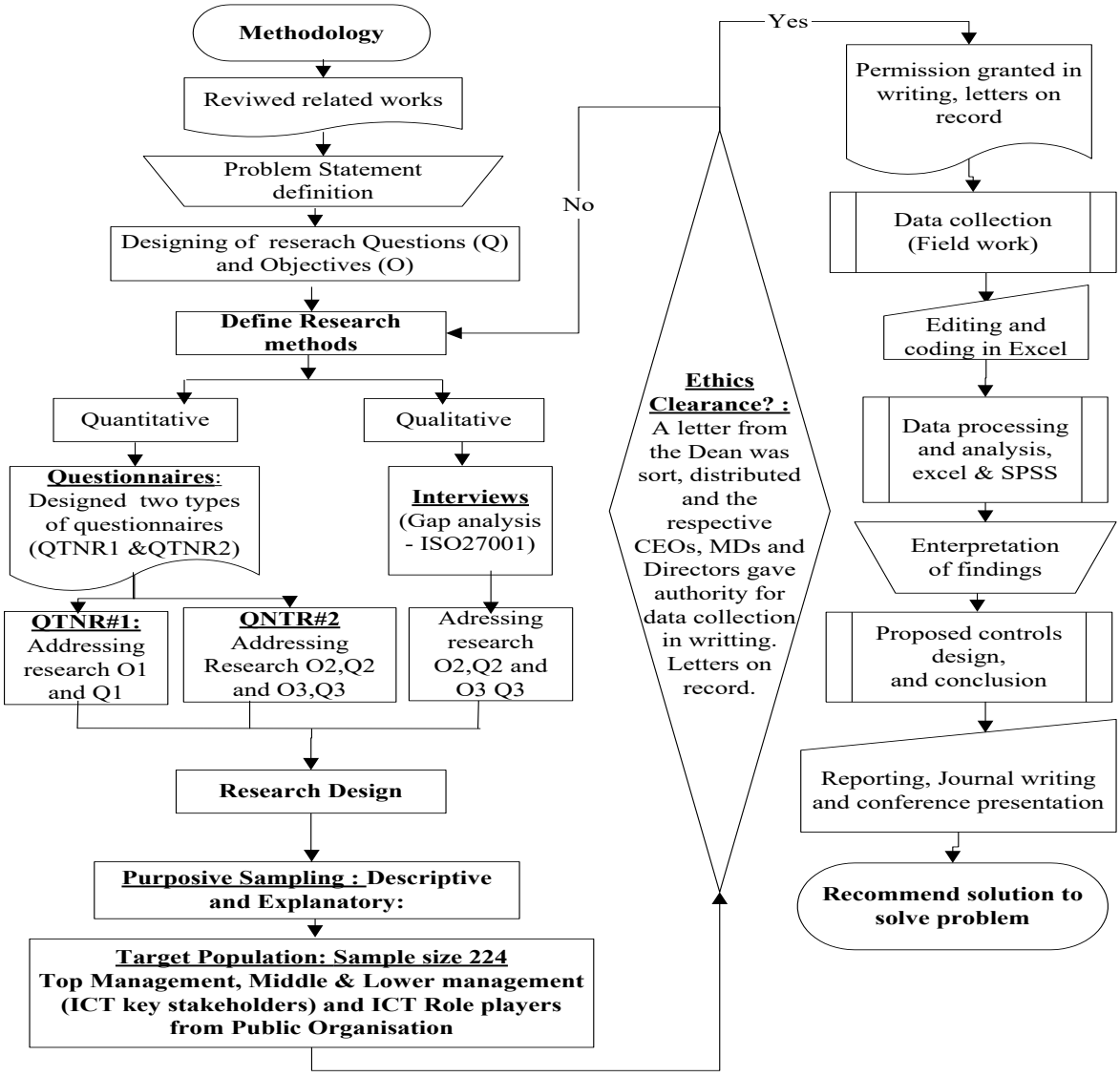


Fig 3.1: Methodology Process Flow chart

3.2 Research Approach

In order to meet the research aim and set out objectives, a mixed approach of both qualitative and quantitative methodologies was employed to investigate, process, analyse and interpret the required information because the study was centered on both deductive and inductive approach. The deductive method involved the design of the theory, research objectives and research questions whereas the inductive method included a detailed analysis of various sources of relevant data collected to discover relevant literature for the study.

Quantitative research is based on a phenomenon that can be expressed or measured in quantity [54]. The research design uses a wide range of data collecting strategies that includes unstructured, semi-structured and structured interviews [55]. The choice of the strategy is dependent on whether the questions and the expected response categories are preplanned, structured and standardized across different respondent and situations. A balanced choice, helps the researcher limit the potential of bias while maintaining question flexibility and variation [56]. In this study, it was used to produce descriptive information for achieving the set research objectives.

Qualitative is based on a phenomenon that concern quality [54]. It can be used to develop the understanding required for evaluating if a variable is relevant or not to a given problem, situation. The approach uses a variety of data collecting strategies among them being questionnaires [57]. In this study, it was used to investigate, analyses and interpret the required quantitative information to achieve the set objectives above.

The reasons for using the mixed approach included the fact that [58];

i. Results superior evidence can only be achieved when different approaches are used to focus on the same phenomenon and they provide the same results
ii. To supplement ones set of results with another
iii. To discover something that would have been missed if only a qualitative or quantitative approach alone was used.

Mndeme argued that multiple approaches are useful if only they afford better prospects for answering research questions and where they allow one to better evaluate the extent to which research findings can be trusted and inference made from them [59]. Take, for instance, interviews may be a valuable way of triangulating data collected by other means such as questionnaires.

Therefore, the nature and purpose of the research will influence the research method and approach adopted, that's why in this deductive process or reasoning we adopted the missed approach.

3.3 Research Design

This is defined as the blueprint for conducting a study with maximum control over factors that may in interfere with the validity of the findings or a plan that describes the process flow of data to be collected and analysed [60]. The design adopted was descriptive and explanatory of both mixes being qualitative and quantitative.

Descriptive because it is designed to provide a real picture of a situation as it naturally happens. It has been used in evaluating the challenges encountered by public organisations as it relates to insider threats as well as identifying factors that lead to insider threats through the reviewed literature. Explanatory because it involves assessing the level of provision of mitigating factors of the insider threats to Zambia's Public Organisations, investigating the awareness levels of the employees as it relates to insider threats mitigation as well as analyzing how insiders impact on the productivity of the nation. We adopted qualitative and quantitative for triangulation purposes, because it is effective in balancing the choice of the researchers, thereby limiting the potential of biases while maintaining question flexibility and variation [56]. The nature and purpose of the research had influenced the research methodology in terms of location, targeted population, duration, sampling design, data collection and analytical procedures. The study developed a theoretical insider cyber threat mitigation model from the available literature and the research findings.

3.4 Target Population

Population is the total number of units from which data can be collected including people, artefacts, events or organisation [61]. Another researcher defines population as the entire set of people who have some common characteristics as defined by the sampling criteria which was established for the study [60].

In this study the population of informants from whom a sample was selected to participate in data collection were Public institution employees whose roles, responsibilities and accountabilities relates to ICT including but not limited to all ICT/Cyber security key stakeholder categories from Executive or Top Management, Middle & Lower management to ICT Role players in eight public organisations. The eight public organisations were picked from various sectors that embraces ICT as a support service to the business units that included; Finance, Banking, Energy, Higher institution of learning, Government Agencies as well as Authority and regulatory boards.

3.4.1 Top Management

These are the executive management that included the CEO's and Directors who are the key sponsors of their various organisational ICT/Cyber security management. They were targeted from a total of eight public institutions because they are the are accountable for the management of ICT/Cyber Security as well as risks of the corporations and they are the most affected be the prevailing insider threats. For the security program to be effective, the projects requires full

support and buy-in from the Executive Management in committing support to ICT/Cyber Security management by approving;

i. Cyber and ICT security related budgets, policies and procedures
ii. Full adoption of international standard and framework like ISO27001 or COBIT 5, implementation and compliance reviews
iii. ICT risks integration into the organisational Enterprise Risk Management (ERM) program
iv. Inclusion of ICT security in all ICT related projects and developments for security compliance purposes.

When research is conducted on Zambia's public organisation with a justified representation of this category forms a basis for generalization and conclusion of the Zambian public organisation position. Therefore, having considered a reasonable sample representative of this population, the research has well represented Zambia's public organisations.

In an endeavor to achieve reliability and validity of data collected, other categories, professions and workmen were engaged through structured questionnaires and interviews.

3.4.2 Middle Management

These are process and function owners who includes departmental heads, managers and supervisors from ICT, Cyber Security, Physical security, Legal, HR and Training, Finance, Internal audit/Risk and Procurement departments. They were targeted because they own assets, processes and functions and manage all processes and functions that relates to ICT/Cyber security. They have a mandate to protect the organisation's information. They are also in charge of managing and coordinating the employees' activities and ensuring ICT/Cyber security compliance from the users and all insiders to the laid policies and procedures.

3.4.3 Lower Management

These included Engineers, officers, administrators, technologists, technicians, analysts and Helpdesk staff from ICT, Cyber Security, Physical security, Legal, HR and Training, Finance, Internal audit/Risk and Procurement departments. They were targeted because they are the ones who are fully involved in the administration of users, data, systems, access rights, employees, contracts, personally identified records and actual classified data handling in public organisations supervised by relevant middle management professionals. They have vast experience in the principal insider related activities and thereby making them resourceful in providing reliable data for research consideration.

3.4.4 ICT Role Players

These included all ICT users in the public organisations under review. They were targeted because they are the ones who are fully involved in the day to day use and handling of all categories of information and systems. Additionally these is the category of users who cause most unintentional data breaches due to ignorance and other unintentional reasons that may eventually compromise data security of the organisation. They have access to most of the information that external perpetrators look for and can easily lure them into providing classified credentials to the attackers. They require more awareness and training, which made them resourceful in providing reliable data for research validation. Table 3.1 illustrates the summary of the research target group, sampling method and justification.

Table 3.1: Target group summary

No.	Target group	Sampling method	Justification
1.	Top Management	Purposive sampling	They are key stakeholders who are accountable for organisational data security.
2.	Middle management	Purposive sampling	They are asset owners, data owners, process owner and function owners who are responsible and mandated to protect the organisation information
3.	Lower Management	Purposive sampling	They are fully involved in the administration of users, data, systems, access rights, employees, contracts, personally identified records and actual classified data handling
4.	ICT role players	Purposive sampling	They are fully involved in the day to day use and handling of all categories of information and systems

3.5 Sampling

A sample is a comparatively minor subset of a population that is projected to represent or stand in for, the population in a particular research [62]. It takes off by defining particular groups of components, that is, individuals, groups and organisations. The sample is selected from the study population that is usually referred to as the "target population or accessible population" [60], [63]. The sample selected included that ICT key stakeholder categories included Top Management, Middle & Lower management from ICT, Cyber Security, Physical security, Legal, HR and

Training, Finance, Internal Audit/Risk and Procurement departments and ICT Role players in eight public organisations.

3.5.1 Sampling Process

Sampling is a process of selecting a group of people, events and behaviour with which to conduct a study [60]. In this research, non-probabilistic sampling was employed. This is purposive sampling which is oriented towards the development of ideological knowledge from generalizations of individual cases and population selected from a non-random cross section of operational staffs. In the questionnaire, six factors which are also global indicators of ICT Security culture were used and modified to fit the public organisation [64].

3.5.2 Purposive (Non-Probability) Sampling

Also known as judgmental sampling, it is referred to as purposeful by [65]. This sampling strategy is employed when there is a very large pool of potentially information-rich cases and no obvious reason to choose one case over another. Other researchers describe purposive sampling as an approach of sampling where a researcher purposefully chooses who should be included in the study based on their capability to provide essential data [66],[67]. Therefore, purposive sampling was used to select the representative sample from eight public organisations population of interest. The justification for selecting this approach was due to the fact that it enables the use of a judgmental selection of cases that can preeminently answer the research question(s) as well as meet the objectives.

3.5.3 Sample Size

In research, for a sample size to be representative of the chosen population, should not be less than 5% of the population size [68]. However, since the research had a view of obtaining a larger sample representation percentage was adopted.

Two different types of questionnaires were distributed to the eight public organisations in sets of a total of 34 questionnaires of both types, which included ICT Security Heads of the companies under review to validate the content. The two Questionnaires distributed in eight organisations were 272 in total and completed during one of the ICT Security circle sessions and a total of 240 responses were received of which 16 were spoiled. The remaining 224 responses account for 82.4.5% response rate. Table 3.2 indicates the demographic distribution and categories of the respondents.

Table 3.2: Demographic Distribution of Respondents

No.	Categories of Companies	Sampling Method	Questionnaire 1	Questionnaire 2	Sample Size Totals
1.	Company 1	Non-probabilistic	14	18	32
2.	Company 2	Non-probabilistic	14	18	32
3.	Company 3	Non-probabilistic	13	18	31
4.	Company 4	Non-probabilistic	12	16	28
5.	Company 5	Non-probabilistic	12	16	28
6.	Company 6	Non-probabilistic	11	15	26
7.	Company 7	Non-probabilistic	10	14	24
8.	Company 8	Non-probabilistic	10	13	23
9.	Totals		96	128	224

3.6 Ethical Considerations

The researcher sought authorization in writing from the University of Zambia to Public organisations respective Chief Executive Offices (CEOs), Managing Directors (MDs)s and Director Generals (DGs) Commissioner Generals (CGs) seeking permission for the research data collection. Permission for data collection was granted from eight public organisations and letters are on record. During this study, a relationship with reference to the letter of approval was first established between the researcher and the respondents which created a comfortable environment for them to openly and freely participate. During interviews, consent was sought to take notes during the response sessions. Respondents were also assured of respect and confidentiality. A

covering letter included the statements on the use of data assuring confidentiality and anonymity of the respondents.

3.7 Methods of Data Collection and Instruments Used

Data collection is defined as the precise and systematic way of collecting information relevant to the research sub-problems, using the methods such as interviews, participate observation, questionnaire completion, focus group discussion, narratives and case studies or histories through the use of quantitative methods. Its major purpose is to verify the research questions and hypothesis. The data sources included both primary and secondary data collection which satisfied the study objectives.

3.7.1 Secondary Data Collection

Secondary data sources included published documents and any recordings that relate to the information originally presented previously [57]. The dataset sources included published journals, dissertations/thesis, reports, textbooks, dictionary, internet and related articles. These sources were used to review related works considering the fact that other documents related to this study were written by other authors from various countries.

3.7.2 Primary Data Collection

Primary data is that which is collected on the first-hand basis and original [57]. Both structured interviews and questionnaires were used as primary data collection instruments that facilitated data collection. Questionnaires were administered to the concerned professionals in public organisations while the interviews were conducted with the targeted ICT related departments and professionals. The targeted population included; ICT key stakeholders and role players from Top Management, Middle management, Lower management and others from the public organisation.

3.7.3 Research Instruments

The data collection methods and instruments adopted for the mixed approach of qualitative and quantitative to achieve the objectives of the study included mailed and self-administered questionnaire as well as structured and non-structured interview in all the eight public organisations. These implementations were made by the researcher through the guidance of the supervisor.

3.7.3.1 Questionnaires

A questionnaire has been defined as any written instrument that presents respondents with a series of questions or statements to which they react by writing the answers [69]. Interview-administered and self-administered questionnaires were both used in this research. Both questionnaire comprised of participant's bio-data, open and closed-ended statements about management of Cyber Security threats by Insiders. Insider threats with its factors were identified from the review of the literature in Chapter 2 to inform the questionnaire development. They were used as the most dominant themes and were adopted in this study after well-researched existing validation measures. It was prudent to make use of these factors in the questionnaires in this research. The statements most relevant to the factors which were identified as themes in this quantitative and qualitative study were selected from each measure. This created a composite questionnaire with 91 questions in total including 16 opinionated statements bordering on Organisational ICT Security Culture as illustrated in Tables 3.3, 3.4, 3.5, 3.6, and 3.7.

Table 3.3: Likert Statements assessing the extent to which internal Cyber/ICT Security controls assurance enhances corporate governance

Themes	Questions
Assessing the extent to which internal Cyber/ICT Security controls assurance enhances corporate governance	i. Your organisation has adopted, implemented and enforced the international ISMS standards and framework such as ISO 27001 and COBIT for security. ii. Cyber/ICT Security has a risk-based plan that determines the priorities of the Cyber/ICT Security activity, consistent with the organization's goals. iii. The Chief Cyber/ICT Security Officer (CISO) ensures that Cyber/ICT Security resources are appropriate, sufficient, and effectively deployed to achieve the approved plan. iv. The Cyber/ICT Security activity assist the company in maintaining effective controls by evaluating their effectiveness and efficiency and by promoting continuous improvement v. Cyber/ICT Security Officers check that internal controls exist and are working effectively vi. Cyber/ICT Security Officers are alert to the significant risks that might affect objectives, operations, or resources. vii. Cyber/ICT Security helps in the achievement of the company's strategic objectives. viii. Cyber/ICT Security ensures that there is compliance with laws, regulations, policies, procedures, and contracts by the company ix. Confidentiality and integrity of financial, strategic, and operational information is assured by CISO x. Cyber/ICT Security has greatly helped to safeguard assets and minimize loss at our organisation xi. Cyber/ICT Security carry out ICT risk assessments that has helped Management at our Organisation xii. Cyber/ICT Security at our organisation issue reports in a useful timely? xiii. Cyber/ICT Security staff are given regular in-house awareness and training in security practice standards xiv. Not all Cyber/ICT Security staff at our Organisation have experience and are certified in Cyber/ICT Security profession xv. What is the most positive or negative attribute that Cyber/ICT Security Officers have exhibited?

Table 3.4: Questions assessing the influence of Cyber/ICT Security recommendations on corporate governance

Themes	Questions
assessing the influence of Cyber/ICT Security recommendations on corporate governance	i. The Cyber/ICT Security activity assess and make appropriate and value adding recommendations which are implemented by management on a timely basis to improve the organization's governance processes ii. The Chief Cyber/ICT Security Officer (CISO) communicates results to the appropriate parties timely for consideration iii. Management accepts responsibility for monitoring corrective action on vulnerabilities reported by Cyber/ICT Security iv. The Cyber/ICT Security executive establishes and maintains a system to monitor the disposition of results communicated to management v. Cyber/ICT Security have a clear and positive relationship with management that allows it to communicate openly and confidently without fear of repercussions vi. Management views Cyber/ICT Security function as an impediment to fulfilling its objective on time vii. The Cyber/ICT Security budget includes adequate funds for professional development and the planned use of external experts viii. The degree of response to Cyber/ICT Security report by senior management is satisfactory ix. What is it that Cyber/ICT Security officials should do or should not do to improve its relevancy at your Organisation?

Table 3.5: Likert Statements assessing the independence and objectivity of Cyber/ICT Security activity in the organisation as a mechanism of governance

Themes	Questions
Assessing the independence and objectivity of Cyber/ICT Security activity in the organisation as a mechanism of governance	i. The department has a charter approved by the board that gives it its mandate and independence with a formally defined purpose, authority, and responsibility of the Cyber/ICT Security activity in line with the Mission of Cyber/ICT Security ii. Cyber/ICT Security Officers are professionals and competent to act independently and objectively in the performance of their work. iii. The relationship between Cyber/ICT Security and employees is viable and professional iv. The Cyber/ICT Security activity is free from interference in determining the scope of Cyber/ICT Security, performing work, and communicating results v. Cyber/ICT Security Officers have an impartial, unbiased attitude and avoid any conflict of interest vi. If independence or objectivity is impaired in fact or appearance, the details of the impairment are disclosed to appropriate parties vii. Cyber/ICT Security Officers provide consulting services relating to operations for which they had previous responsibilities viii. If Cyber/ICT Security Officers have potential impairments to independence or objectivity relating to proposed consulting services, the disclosure is made to the engagement client prior to accepting the engagement ix. Cyber/ICT Security function sometimes faces interference from management in determining its scope and communicating results. x. Cyber/ICT Security at our organisation have access to all records and books without interference from line managers xi. Cyber/ICT Security staff are required to review all departments in the organisation xii. Cyber/ICT Security Function report at a very senior level in the Organisation xiii. Cyber/ICT Security have no personal or professional involvement with or allegiance to the asset being protected and maintains an unbiased and impartial mindset in regard to all engagements at our organisation xiv. Is Cyber/ICT Security function seen and act independently at your company? YES or NO.

Table 3.6: Questions assessing the insider threats and security activity in the organisation

Themes	Questions
Assessing the insider threats and security activity in the organisation	i. Which category of insider are you the most concerned with as being the most detrimental to your organization ii. What are you most concerned about as relates to an insider threat? Select all that apply iii. Can you place a financial value in U.S. dollars on your organization's potential loss from an insider threat? iv. Does your organisation have the ability to prevent/deter an insider incident/attack? v. What tools or techniques are you using to prevent/deter insider threats before they become an actual incident or attack? vi. What Administrative policies & procedures are you using to prevent, detect and mitigate actual insider threats incident or attack? Select all that apply. vii. Does your ICT /Cyber Security/HR department mandate a screening and underground check for prospective employees before they are employed? viii. How often do you review the policies and procedure? Select all that apply ix. How often do you conduct user awareness? Select all that apply x. Who is covered under awareness/training scope? xi. What factors do you feel are limiting your ability to prevent/deter an insider incident/attack? Select all that apply. xii. How effective do you feel your prevention measures are? xiii. What tools or techniques do you use to detect insider incidents/attacks? Select all that apply. xiv. Does your incident response plan has special provisions for incidents involving insiders? xv. Have you ever experienced an actual insider incident/attack in your organisation? xvi. From the actual or estimated start of the incident/attack, how long did it take you to detect/mitigate? xvii. What do you estimate was the extent of your (worst) loss in U.S. dollars? xviii. Does your organisation have an ICT/ Cyber Security policy and procedure which are aligned with the corporate strategy? xix. Does your organisation have a mandatory Non-Disclosure Agreements (NDA) Policy? xx. What's the Policy for user access rights deactivation after termination of contract?

Table 3.7: Questions assessing Your Vulnerability to Insider Threats

Themes	Questions
Assessing Your Vulnerability to Insider Threats	i. Why do you think an insider would attack their own employers? ii. What do you think would lead to insider attack in your organisation? iii. Which of the indicators has your organisation adequately addressed in mitigating insider attacks? iv. What information would an adversary target in your organisation? v. What systems contain the information that attackers would target? vi. Who has access to the critical information and systems? vii. How would an adversary target that individual? viii. What would be the easiest way to compromise an insider in your organisation? ix. How would someone extract the information? x. What measures or solutions should your ICT use/put in place to prevent these attacks? xi. What measures or solutions can ICT use to detect these attacks? xii. What gaps exist in how you are dealing with insider threats in your organisation? xiii. What are the highest-priority items/assets to focus on? xiv. Does our current budget appropriately address insider threats? xv. Should your organisation adjust current resources and budget to address insider threats? xvi. What would a security roadmap that includes insider threats look like? xvii. I attend at least one awareness training in a month on procedures.

Advantages of Questionnaires

Questionnaires were used due to the following advantages [70], [71].

a) **An Easier Method -** A questionnaire is comparatively an easier method to plan, construct and administer. It does not require much technical skill or knowledge.

b) **Uniformity -** It helps in focusing the respondent's attention on significant items. As it is administered, in a written form, its standardized instructions for recording responses ensure some uniformity. The questionnaire does not permit variations.

c) **Greater Validity -** Questionnaires have some unique merits as regards the validity of the information. In methods like interview and observation, the reliability of responses depends on the way the investigator has recorded them. In the questionnaire method, the responses given by the subjects are available in their own language and version. Therefore, it cannot be wrongly interpreted by the researcher.

d) **Repetitive Information -** Compared to other methods like interviews or observations, using a questionnaire is regarded as more useful and cheap, where the repetitive information has to be collected at regular interval.

e) **Wide Coverage -** Questionnaires make it possible to make contact with many people who could not otherwise be reached. It can cover a large group at the same time. When the researcher has to cover the group of respondents who are widely scattered, they can use the questionnaire in order to minimize the cost.

f) **Economical -** It is an economical way of accumulating information. It is economical both for the sender and for the respondent in time, effort and cost. The cost of conducting the study with the help of the questionnaire method is very low. By using a questionnaire the researcher can only spend on paper printing and postage. There is no need to visit each and every respondent personally, hence it does not require a high cost to conduct of the research.

g) **Suitable in Special Type of Response -** The information about respondents and any secret matters can be best obtained through questionnaire methods. For example, information about the sexual relationship, marital relationship, secret desires etc. can .be easily obtained by 'keeping the names of the respondents anonymous.

h) **Rapidity -** Replies may be received very quickly when using a questionnaire as a means of data collection method. In this case, there is no need to visit the respondent personally or continue the study over a long period. Therefore in comparison with other methods, the mailed questionnaire is the quickest method.

i) **Anonymity -** A questionnaire ensures anonymity to its respondents. The respondents have high confidence that they will not be identified by anybody for giving a particular view or opinion. They feel more comfortable and free to express their view in this method.

Disadvantages of Questionnaires

The following are some of the disadvantages of using a questionnaire for data collection, which the researcher was very mindful of [65];

a) Questionnaires are standardized so it is not possible to explain any points in the questions that participants might misinterpret
b) Open-ended questions can generate large amounts of data that can take a long time to process and Analyse
c) Respondents may answer superficially especially if the questionnaire takes a long time to complete
d) Respondents may not be willing to answer the questions.

Applicability

We used questionnaires due to the above advantages and the fact that they were less costly, easy to administer, reduced n the potential interviewer biases, convenient, useful for future references and allowed the flexibility in time for answering.

3.7.3.2 Interviews

Interviews refer to the structured and unstructured verbal communication between the researcher and the subject in which information is presented [60].

Structured interviews use questionnaires based on a predetermined and standardized or identical wet of questions known as interviewer-administered questionnaires. During the interview, each question is read out and the response is recorded on a standardized schedule usually with pre-coded answers [60].

Advantages of Interviews;

The interview was used due to the following advantages [60]:

a) Permits face to face contacts with the respondents
b) They usually produce the richest data and new insights
c) Provide an opportunity to explore topics in depth
d) Allow the interviewer to experience the effectiveness and the cognitive aspect of the responses

e) Allow the interviewer to be more flexible in administering interview to a particular individual in a particular circumstance
f) Allow the interviewer to explain and help clarify questions, increasing the likelihood of useful responses.

Applicability

These structured interviews were used to obtain information from the respondents that could easily be reached and have a meeting arranged with meanwhile the unstructured interviews were used with the view to obtain answers to questions that require respondents to give detailed but yet extensive explanations.

3.8 Methodology Reliability

Reliability is the degree to which outcomes are consistent over time and a precise depiction of the total population under the study and if the results of a study can be reproduced under a similar approach, then the research instrument is considered to be reliable [53]. Consequently, in warranting the reliability of the data collected in this research, similarly, structured questionnaires were administered and sought respectively among Departmental heads, managers, supervisors, professionals and role player's employees from the eight public organisations. This was done to ensure dependability in the data collected making the research reliable [53].

3.9 Methodological Validity

Validity is the best available estimate to the truth or falsity of a particular interpretation, proposition or decision [71]. It indicates the extent to which the research measures what it purports to measure hence indicating how complete the research is through the design and methods adopted [72]. The two types of validity known include; internal and external. Internal validity refers to whether the study sufficiently describes the phenomenon it sets out to examine, in the ability to draw conclusions from observations; while external validity refers to an inference of the pivotal connections of the research findings and the extent to which they can be generalized [45], [73]. Hence, the validity of the data collected is meant to minimize measurement error, bias, and enhance the thoroughness of the research findings and their interpretability.

This study was therefore externally valid because the findings could only be extended or applied to the public organisations within which the study took place. Furthermore, the respondents were not pressured in any way to select specific choices among the answers given from the

questionnaires. Therefore, the validity of the research was achieved since the findings truly represent the phenomenon being claimed to be measured.

3.10 Data Organisation, Processing, Analysis and Presentation

3.10.1 Data Organization

After collecting all the questionnaires, data was organized in order by going through each questionnaire checklists, scrutinizing each question and their responses in order of response. This helped to eliminate the unusable data, interpretation of unclear answers and identification and correction of errors.

3.10.2 Data Processing

Processing included the coding and entry were done manually using the Microsoft Excel and was further processed, analysed and tabulated using the computer Statistical Packages for Social Sciences (SPSS). One researcher conceived suggestions that a detailed study contains features such as the systematic collection and interpretation of data including a more clear purpose of judgement [53]. They also contended that research should involve a clarification and explanation of methods and approaches used to collect data, an argument as to why the results obtained are valid, and an explanation of any limitations associated with them [53].

3.10.3 Data Analysis

Data analysis refers to the computation of certain measures along with searching for patterns of relationship that exist among data – groups [71]. Once the pattern has been identified it is interpreted in terms of a social theory or the setting I which it occurred and the qualitative researcher moves from the description of the historical event or social setting to a more general interpretation of its meaning [74]. In this study, data analysis consisted of the examining, categorising, tabulating, testing and combining both the qualitative and quantitative evidence so as the address the initials propositions of the study [75]. Frequency distribution, a data analysis technique which allows a researcher to get a big picture of the data from the frequency distribution was adopted, so as to see how the frequency of specific values are observed and what percentages are of similar variables [52].

3.10.4 Data Presentation

Data presentation took the form of histograms, pie charts and graphs. This was achieved using Microsoft excel and word for the presentation of the collected results. All collected data from the fieldwork was considered as the findings and was analysed accordingly.

i. **Quantitative:** This was based on the arithmetical application through the statistical analysis, and was presented using the percentages, bar charts and pie charts for simple descriptive display of the categorical data with no emphasis on the percentage of a total representation by each category.
ii. **Qualitative:** This gave the researcher an interpretative character. It helped to get the information through the descriptive analysis and to explain the findings in detail relative to the existing literature.

3.11 Limitation

The limitation to the research was due to the sensitivity of the research topic that some public institutions did not approve of the data collection application.

3.12 Chapter Summary

This chapter outlined the research approach in which the method and procedures for administering the questionnaires, data collection and analysis was also discussed including statistical methods namely descriptive statistics. It further discussed the sample size, sampling processes as well as the justifications which were employed before considering the data collection approach, instruments, methodological reliability and validity of various techniques used in this study. The methodology adopted for this research was accomplished by the appropriate research approach, design and target population. Furthermore, the approach and tools of data collection employed have been discussed thoroughly together with appropriate research procedural reliability and validity concerns.

CHAPTER FOUR

FINDINGS AND DATA PRESENTATION

4.1 Introduction

The preceding chapter discoursed the following areas; research methodology adopted for this study to fulfil the research objectives as set out in chapter one, research approach, research design, research population, sample and sampling process and justification. This is significant as it provides the basis on which the findings of the research could be generalized and authenticated. The findings assist the practitioners, management and workers to entrench an ICT/Cyber Security culture. This chapter presents findings of this research.

4.2 Background to the Findings

The information that was obtained from respondents during the field research is presented and analysed so as to draw conclusions and recommendations for the research. The presentation of findings was aimed at meeting the overall objectives of the study which is to an investigation into Cyber Security threats posed by insiders: a case of public organisations and to answer the research questions.

4.3 Response Rate

The total number of questionnaires distributed were 272 (100%) rate. Only 240 (88.2%), questionnaires were received of which 16(5.9%) were spoiled, the remaining 32 (11.8%) questionnaires were not received and the remaining 224 responses account for 82.5% successful response rate as indicated in Fig 4.1.

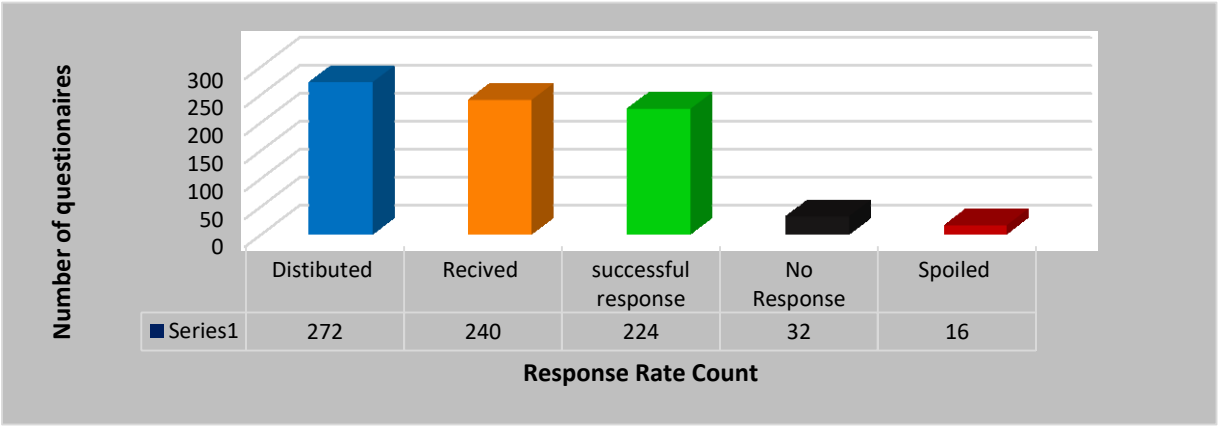


Fig 4.1: Distributed questionnaires and respondent rate

Table 4.1: Summary of the sample sizes and response rates

No.	Categories of Companies	Sample size totals	Spoiled plus non responsive	Successful Response	Response Rate
1.	Company 1	34	2	32	94.1%
2.	Company 2	34	2	32	94.1%
3.	Company 3	34	3	31	91.2%
4.	Company 4	34	6	28	82.4%
5.	Company 5	34	6	28	82.4%
6.	Company 6	34	8	26	76.5%
7.	Company 7	34	10	24	70.6%
8.	Company 8	34	11	23	67.6%
9.	**Totals**	**272**	**48**	**224**	**82.4%**

A total of 272 employees from 8 public organisations were drawn from various professionals and departments of interest. The drawn samples are as summarized in Table 4.1 were a total of 272 questionnaires were administered and the overall response was 224 giving us a general response rate of 82.4%.

Fig 4.2 presents the major roles of the respondents whose responsibilities have a direct effect on the insider threats.

Fig 4.2: Roles of respondents.

Types Of Threats

The pie chart in Fig 4.3 shows the common types of threats posed by insiders in the three organisations under review.

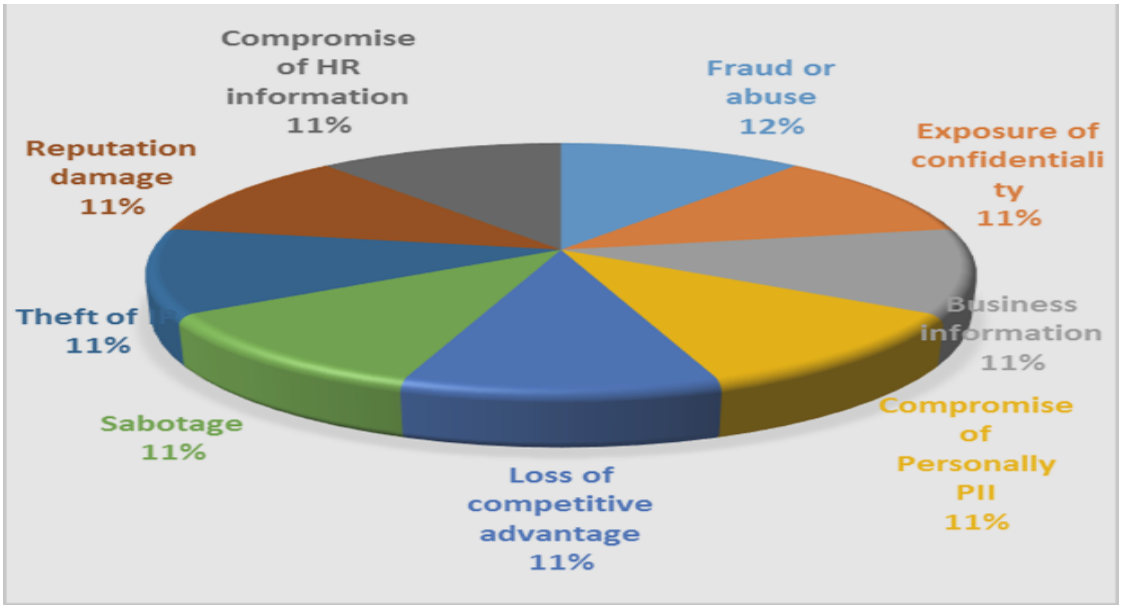


Fig 4. 3: Types of Insider threats.

Categories of Insider Actors

The pie chart in Fig 4.4 show the common categories of insider threat actors in the three organisations under review.

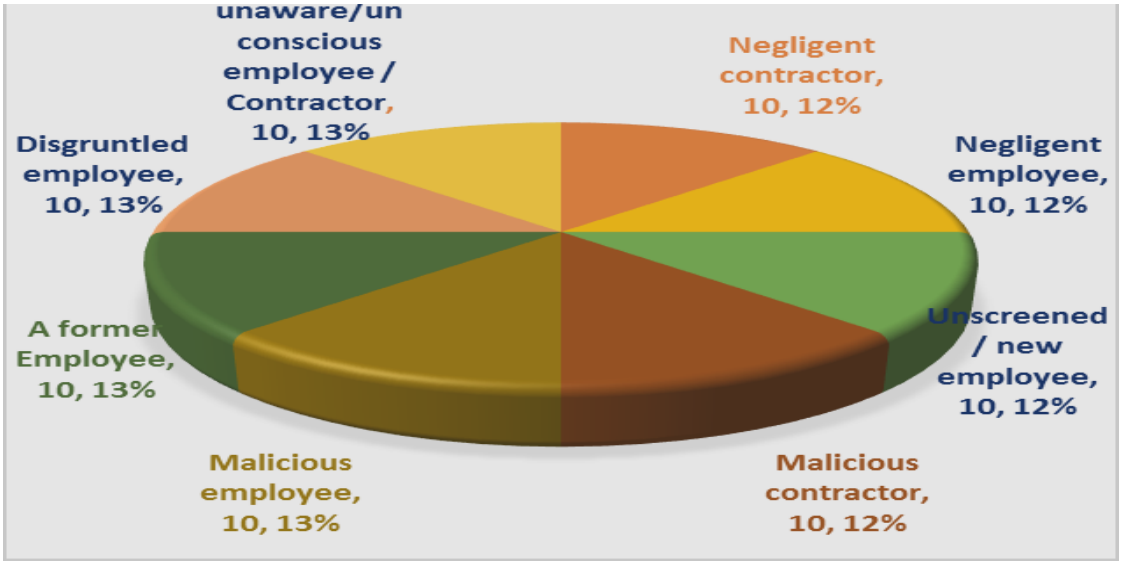


Fig 4.4: Categories of insider actors

4.4 Interpretation of Findings

4.4.1 Recognition of the need for ICT/Cyber Security departments in Public Organisations

4.4.1.1 Availability of Cyber/ICT Security department

An assessment was carried out to ascertain the current levels of Cyber Security awareness and readiness in Zambia Public organisations by means of ICT/Cyber Security department and staff establishment. The findings were as shown in the Figs 4.5 and 4.6.

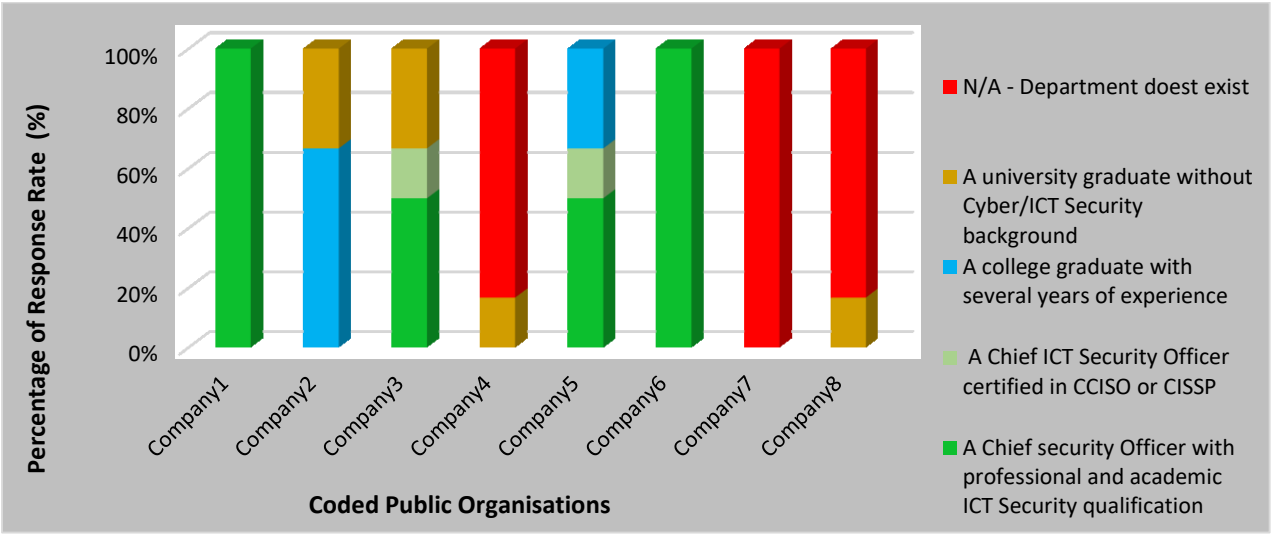


Fig 4.5: Availability of Cyber/ICT Security department and competency of the departmental head.

4.4.1.2 ICT/Cyber Security Staff Establishment

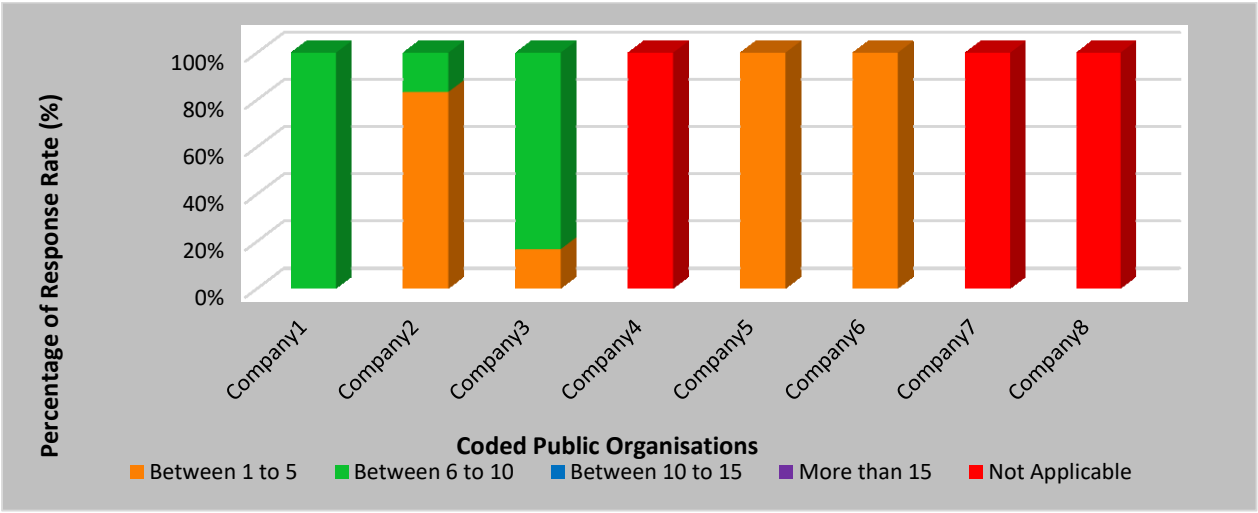


Fig 4.6: The number of staff in the Cyber/ICT Security department/Section at your organisation

The research revealed that only five (5) organisations had a seemingly acceptable number of ICT/Cyber Security staff to help mitigate the cyber threats including insiders. However, through interviews, the research established that of those organisations who have ICT/Cyber Security staff only three (3) had qualified ICT/Cyber Security staff. Further out of the three, only two (2) had an average number of staff being between six (6) to ten (10) in total as shown in Fig 4.6, to cover the organisations' security requirements on average.

4.4.1.3 Executive Management's Buy-In And Support for the Cyber/ICT Security Department

An assessment was carried out to ascertain the levels of Cyber Security buy-in, support and funding by top management, so as to ensure Cyber Security readiness in Zambia Public organisations. The findings were as shown in the Figs 4.7, 4.8 and 4.9.

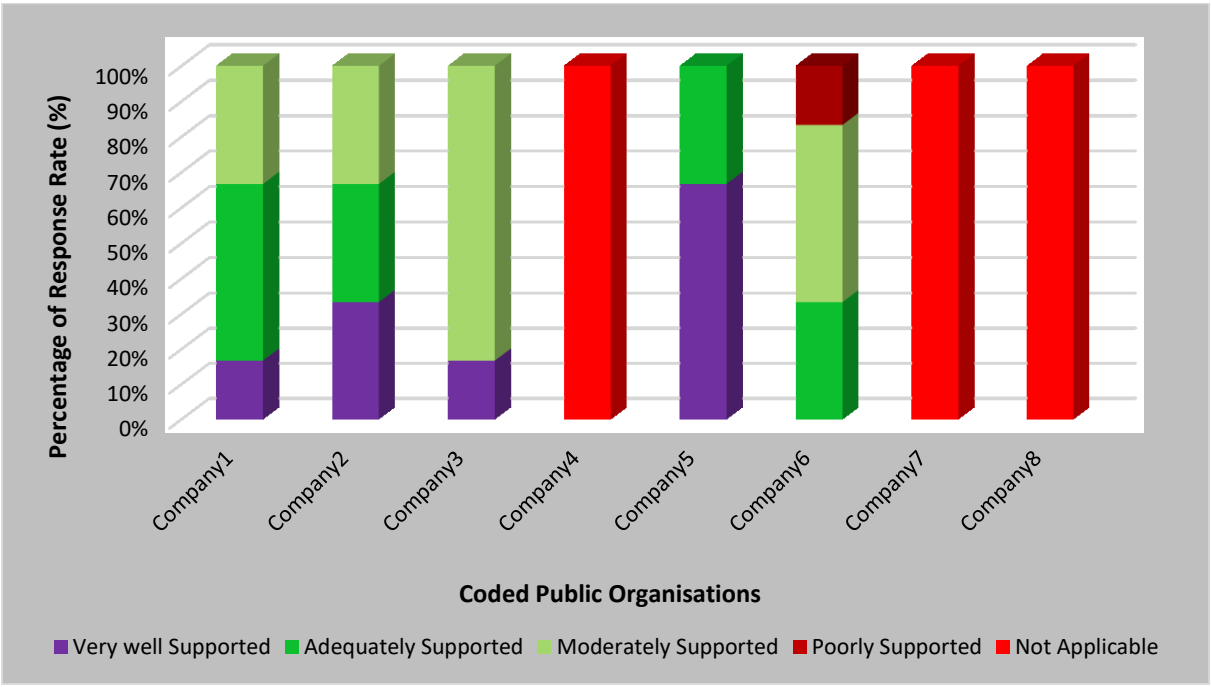


Fig 4.7: Cyber/ICT Security department buy-in and support by the executive management

The research revealed that only five (5) organisations had average management buy-in and support as in Fig 4.7.

4.4.1.4 Executive Management's funding of the Cyber/ICT Security Department Projects.

Statistics for Funding were similar to the buy-in and support, that revealed the same five (5) organisations which had average management buy-in and support are the same organisations that

were between well and moderately funded as in Fig 4.6. However, through interviews, the research established that despite some organisations having executive's partial support, the departmental budgets are never approved as is required of the department, because management feels its unnecessary cost. Majority of the few that approved budgets still were only allowed to less than 10% of the ICT budget as shown in Figs 4.8 and 4.9. Thereby making the management of insider Cyber Security threats a night mere.

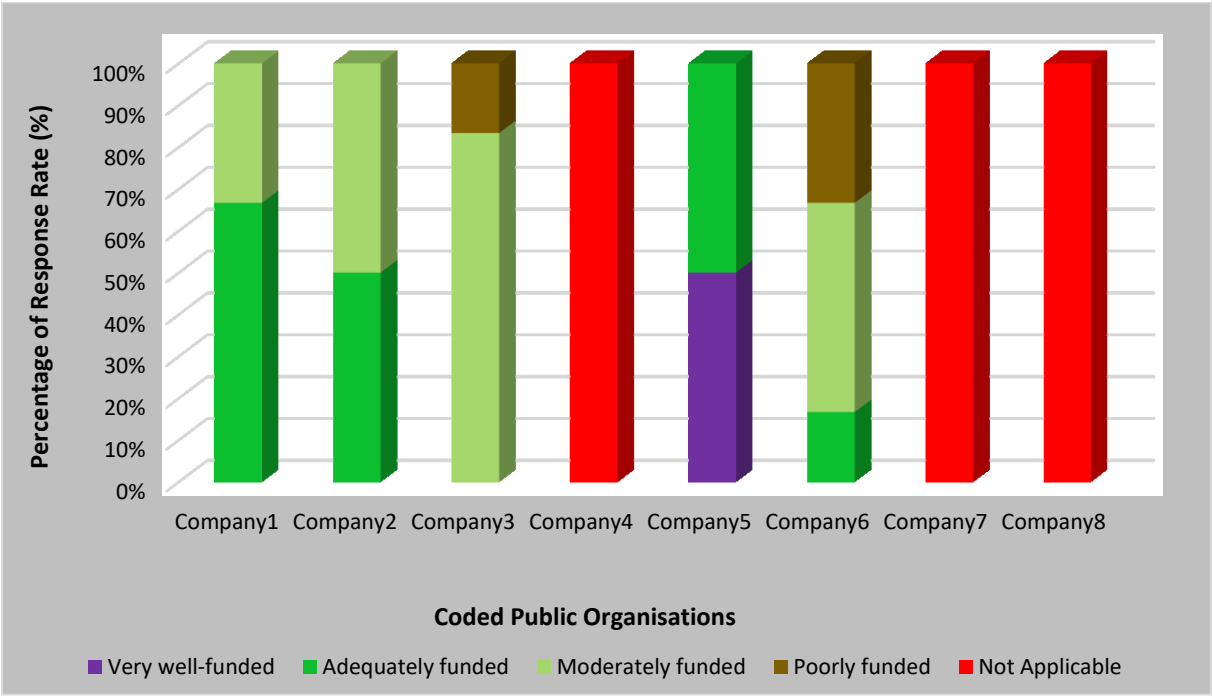


Fig 4.8: Cyber/ICT Security department funding by the executive management.

4.4.1.5 The Percentage ICT Budget Currently Spent on Prevention and Detection of Insider Incidents/Attacks.

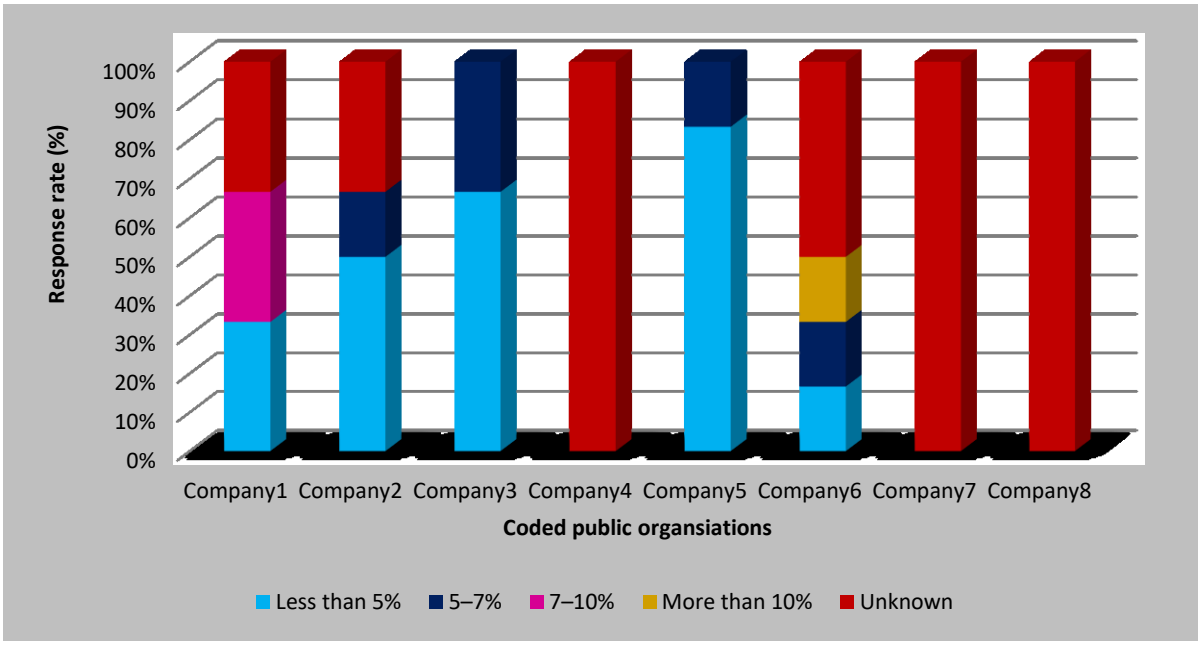


Fig 4.9: Budget of the ICT, spent on mitigation of insider threats.

4.4.2 Results Addressing the Research Objectives and Questions

4.4.2.1 Types of Vulnerabilities That an Insider Can Exploit In Public Organisation.

In addressing research question one (1), an assessment was carried out to establish the types of vulnerabilities in public organisations that can easily be exploited by an insider. The findings were as shown in Fig 4.10. The research findings revealed 24 vulnerabilities common among public organisations that an insider can exploit and breach data security. With the most common seven giving above 70% response being Fraud, exposure of confidentiality, Sabotage, lack of training, lack of policies and procedure, technology complexity and lack of insider threat administration. These vulnerabilities require immediate attention. However, public organisations have challenges meeting the international frameworks and standards because of the high cost of implementing them.

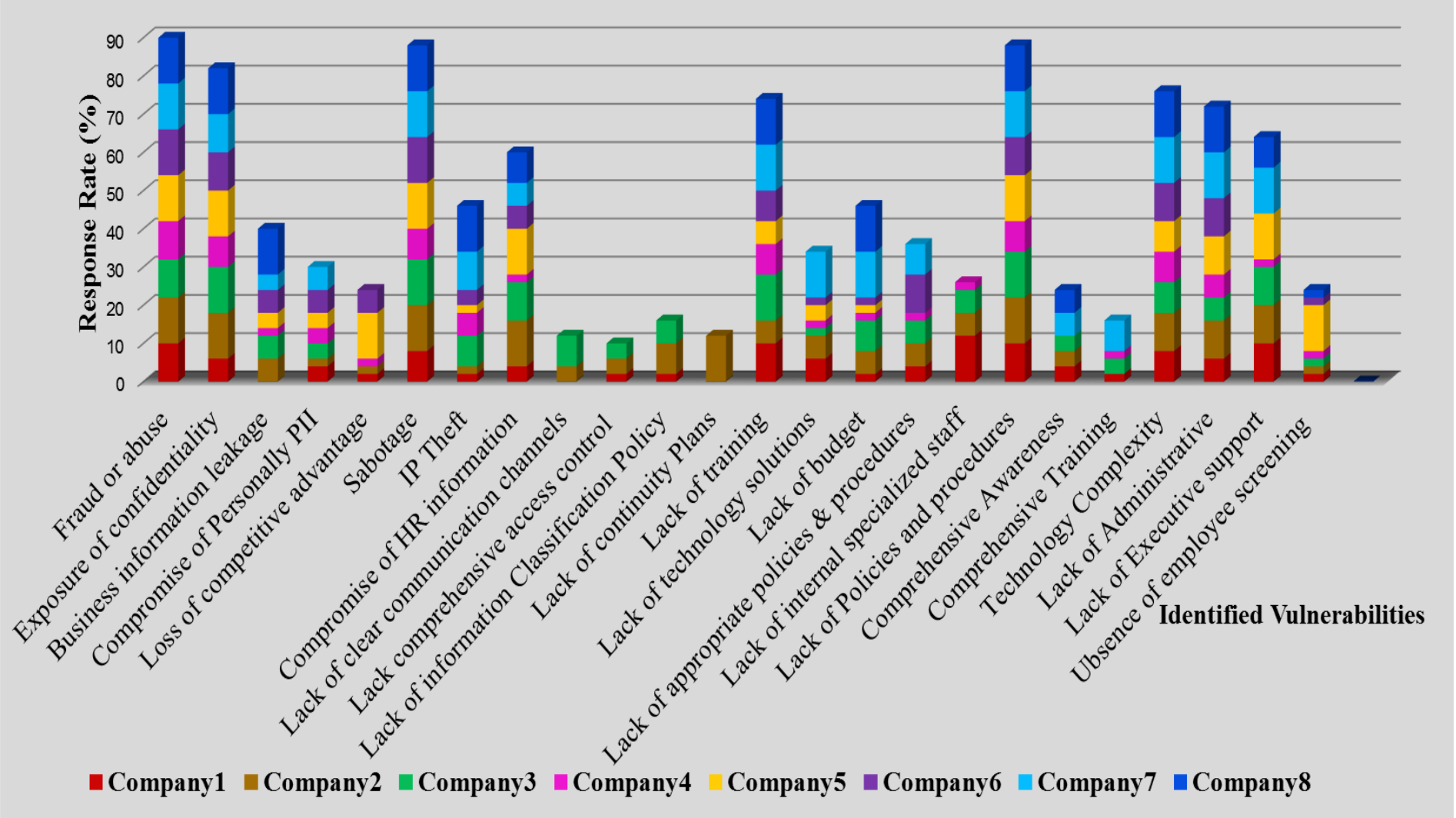


Fig 4.10: Types of Vulnerabilities identified in public organisations.

4.4.2.2 Effectiveness of the Current Controls

In addressing research question two (2), a number of assessments including control analysis and verification were carried out to establish the effectiveness of the current controls as it relates to insider threat mitigation. The findings were as shown in Fig 4.11 through to Fig 4.19.

4.4.2.2.1 Insider Attack Experience

The research findings revealed that all the eight organisations under study have experienced cyber security threats by insiders. This ascertained the effectiveness of the current controls employed in public organisations to curb and or mitigate insider threats. The statistics are as shown in Fig 4.11.

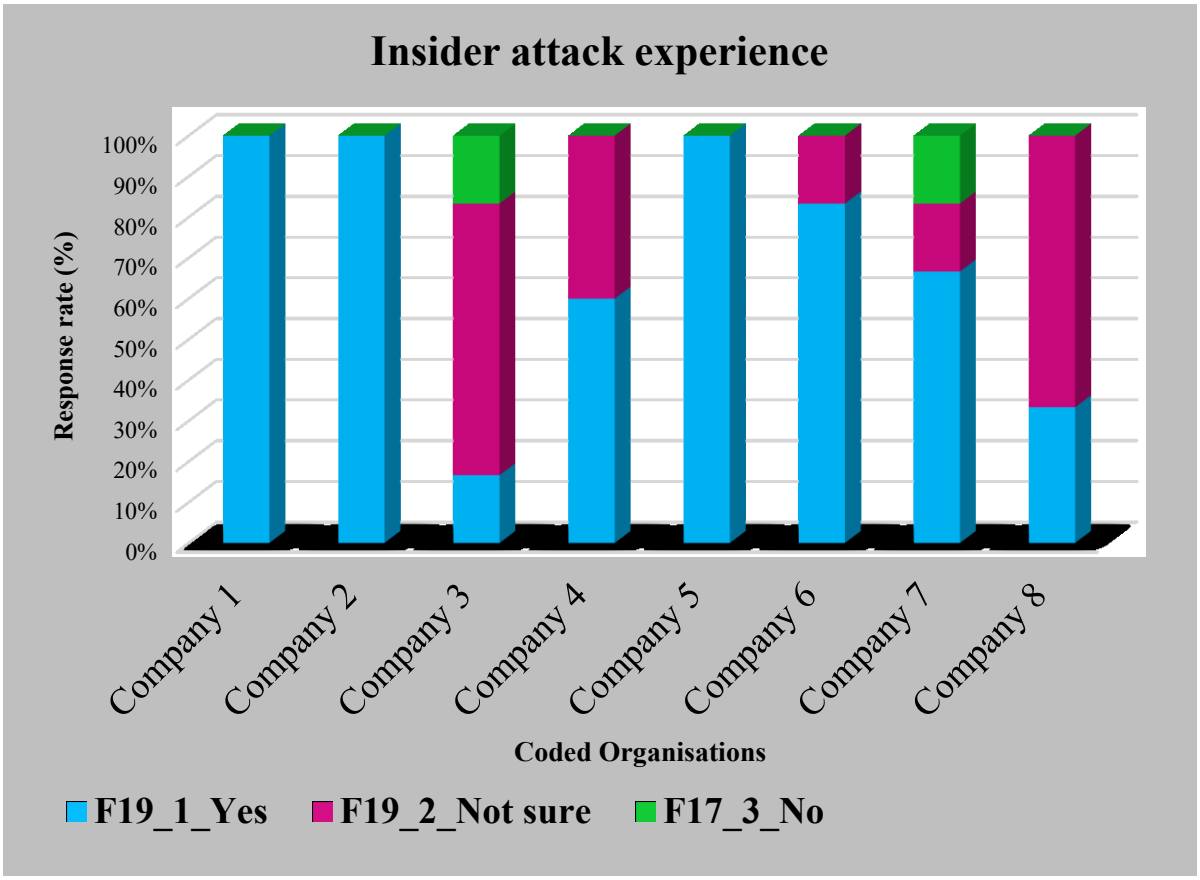


Fig 4.11: Companies suffered insider attacks

4.4.2.2.2 Estimated Cost of Loss Due to Insider Attack

The findings revealed that all the targeted organisations have recorded insider attacks incidences with a recorded loss of funds ranging to more than five million dollars (USD 5M). The current controls were found to not be effective enough to mitigate insider threats to an acceptable level. More than 50% of public organisations investigated, only had partial ICT security-related policies and procedures in place. Nonetheless, the documents are not known to the role players who are in turn expected to comply in order to ensure data security. Meanwhile, about 25% of the organisations were found to not have an ICT/Cyber Security department or ICT/Cyber Security specialized staff to effect the security controls. The statistics are as shown in Fig 4.12.

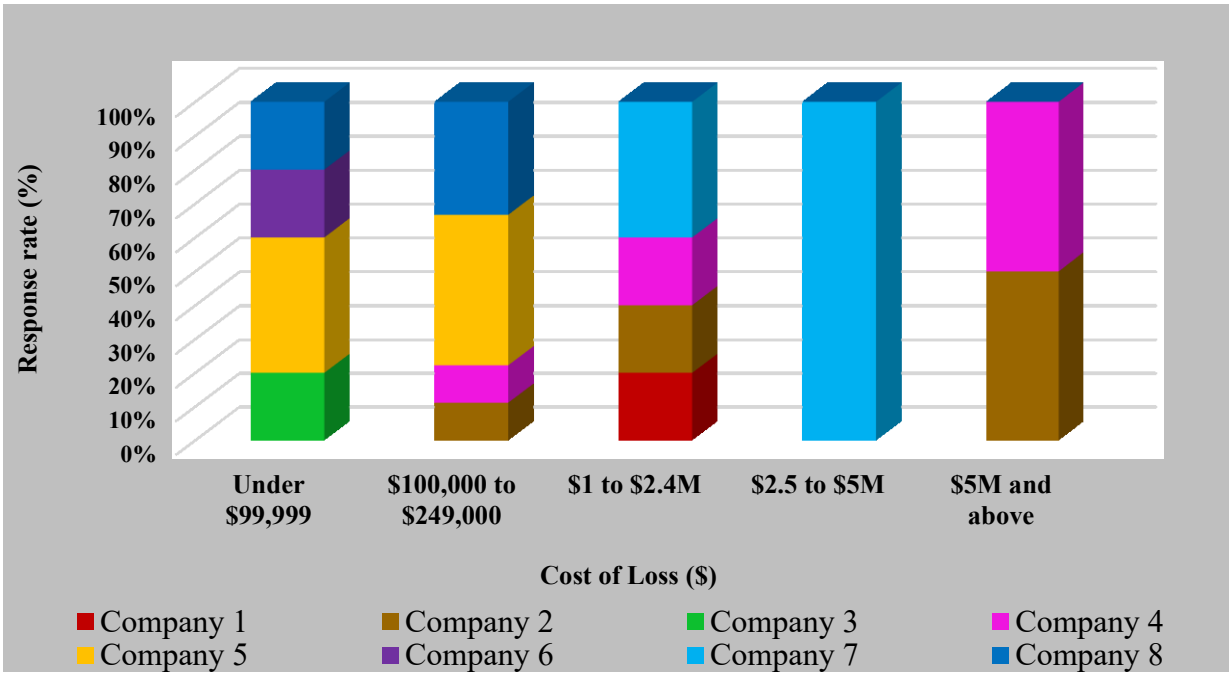


Fig 4.12: Insider attack cost

4.4.2.2.3 Status of the Administrative Policies & Procedures

The research revealed the common policies and procedures that are used by most public organisations though they are not fully implemented and or adhered to in preventing, detecting and mitigating actual insider threats incident or attack per company. The statistics are as shown in Fig 4.13

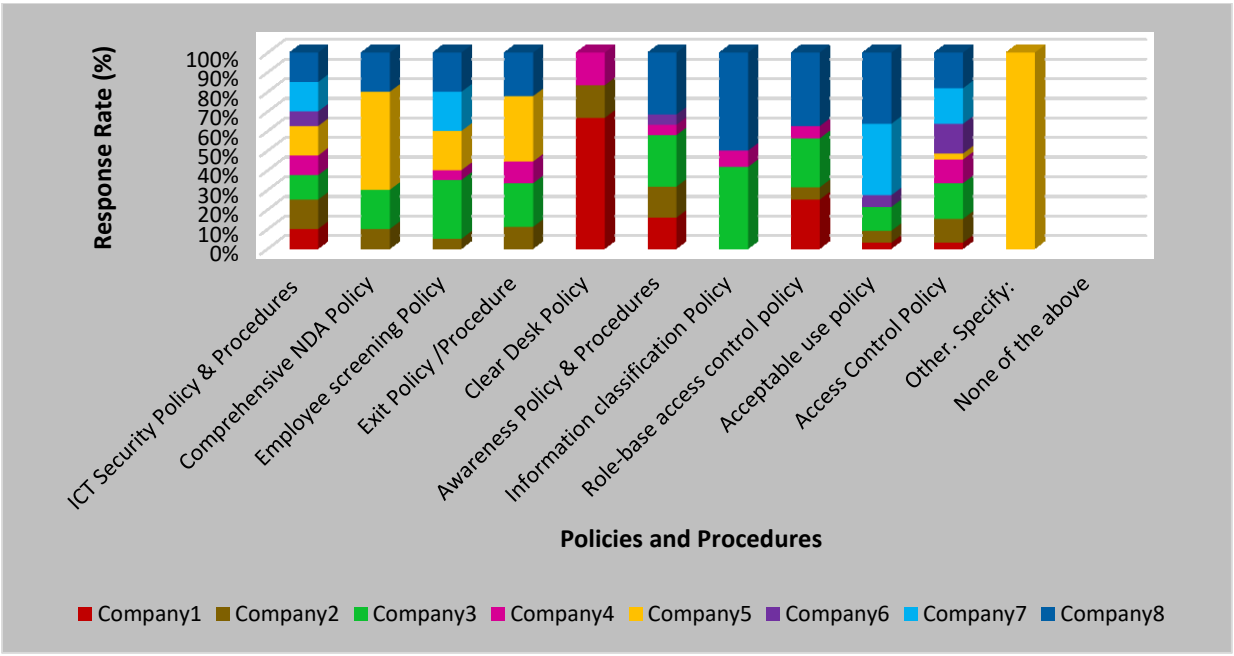


Fig 4.13: Administrative policies & procedures use for insider prevention.

4.4.2.2.4 Mandatory Screening and Underground Check for Prospective Employees.

The research revealed that majority (being five out of eight) of the public organisations under study, do not have an ICT /Cyber Security and HR screening policy for new employees and contractors, before they are employed. This poses a high risk in the management of Cyber security threats by insiders. The statistics are as shown in Fig 4.14.

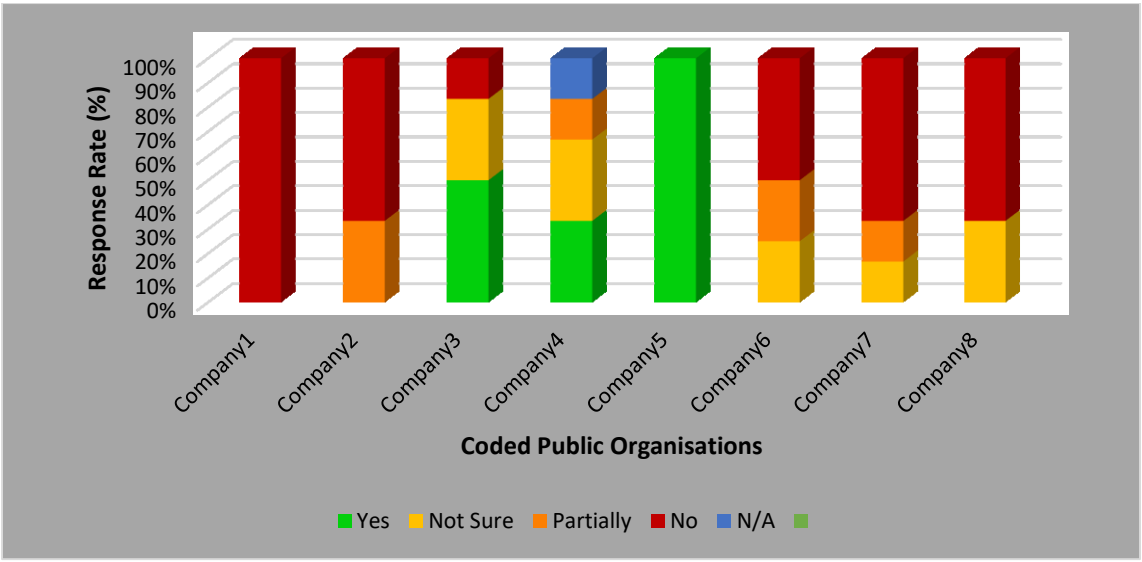


Fig 4.14: Status of organisational mandatory screening and underground check for prospective employees.

4.4.2.2.5 Organisation with a Mandatory Non-Disclosure Agreement (NDA) Policy.

The research revealed that majority (being five out of eight) of the public organisations under study, do not have a mandatory NDA policy with deliberate clauses to deter the exiting employees or contractors from leaking the organisational information and sabotaging the organisation to deter the prospective perpetrators from compromising the security of their employers assets. This poses a high risk in the management of Cyber security threats by insiders. The statistics are as shown in Fig 4.15**.**

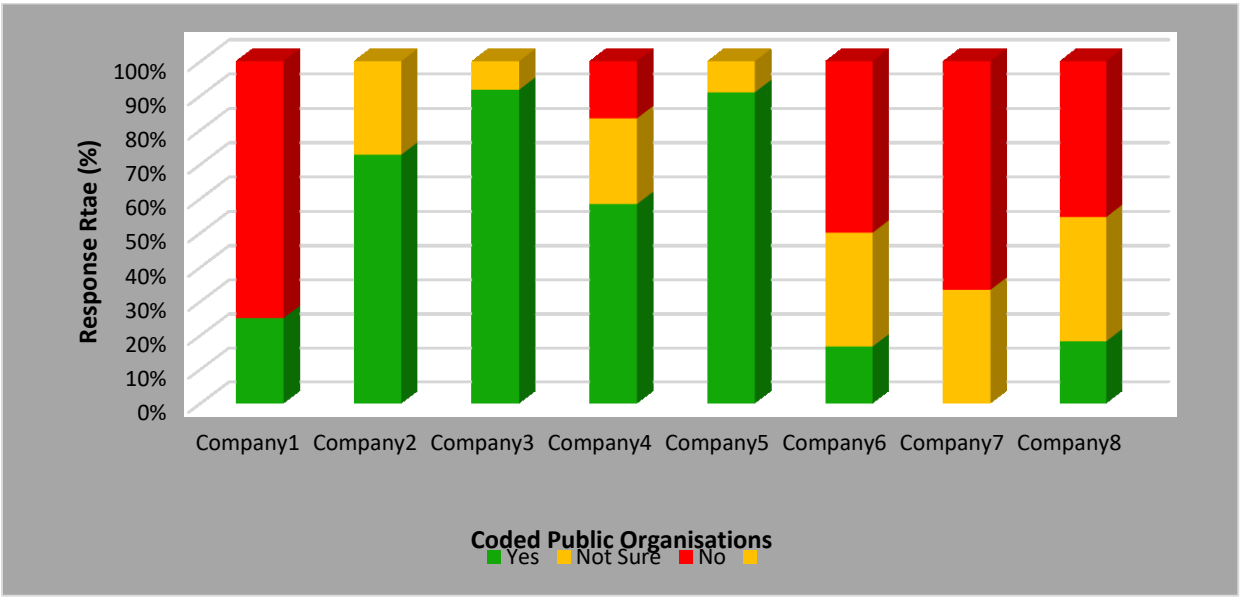


Fig 4:15 Status of NDA availability in public organisations

4.4.2.2.6 Incident Response Plans' Special Provisions for Insider Related Incidents.

The research revealed that most of the public organisations under study, do not have a incident management systems that includes insider threats to manage the cyber security incidences and learn from them. This poses a high risk for business continuity and management of Cyber security threats by insiders. The statistics are as shown in Fig 4.16**.**

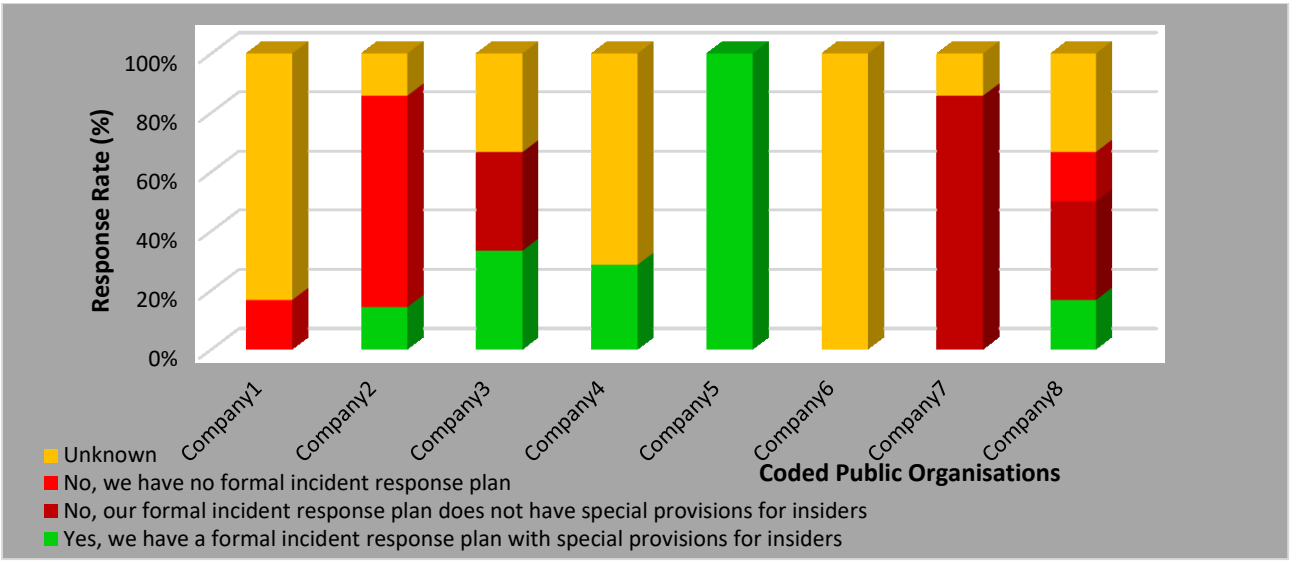


Fig 4.16: Status of organisational incident management systems that includes insider threats.

4.4.2.2.7 Effectiveness of the Current Controls in Addressing Insider Threats.

The research findings revealed that the current controls employed in public organisations to curb and or mitigate insider threats are not effective enough to mitigate the threats to an acceptable level. This was supported by the response from the control questions that were set to ascertain the claimed effectiveness by the public organisations as shown in Fig 4.17.

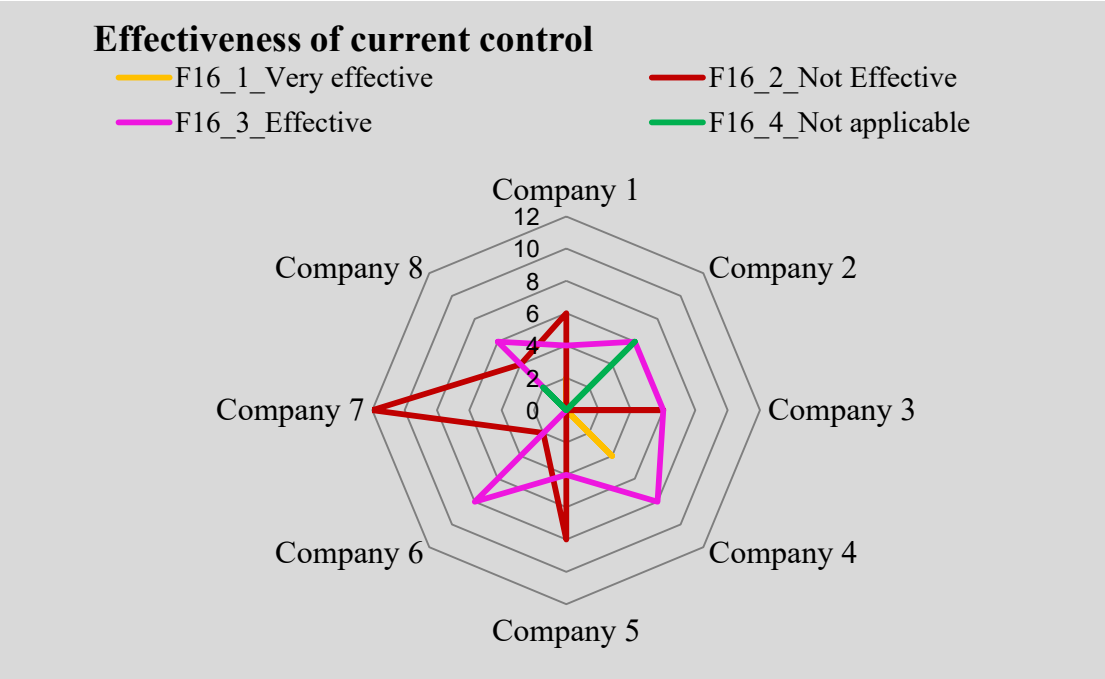


Fig 4.17: Effectiveness of the current controls.

4.4.2.3 ICT/Cyber Security GAP Analysis so as To Propose an Ideal Mitigation Model

In addressing research question 3, a gap analysis based on ISO 27001:2013 standard was carried out to establish the gaps in the current ICT Security controls so as to be able to possibly recommend mitigating measures to insider threats that will be in tandem to the International standard ISO 27001:2013 that can address the issues in question (i) and (ii) above. The findings were as shown in Fig 4.18, through to Fig 4.22

4.4.2.3.1 ICT Security Implementation Processes

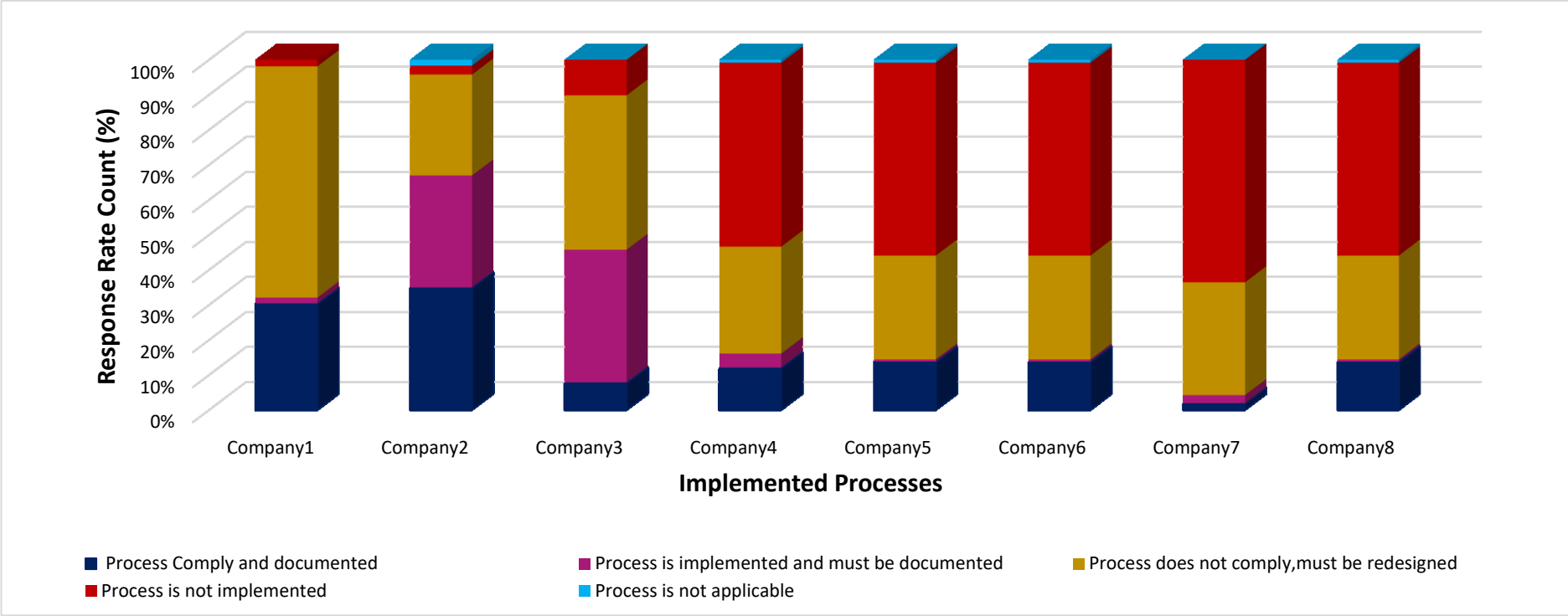


Fig 4.18: Status of implemented processes

4.4.2.3.2 ICT Security Implementation Controls

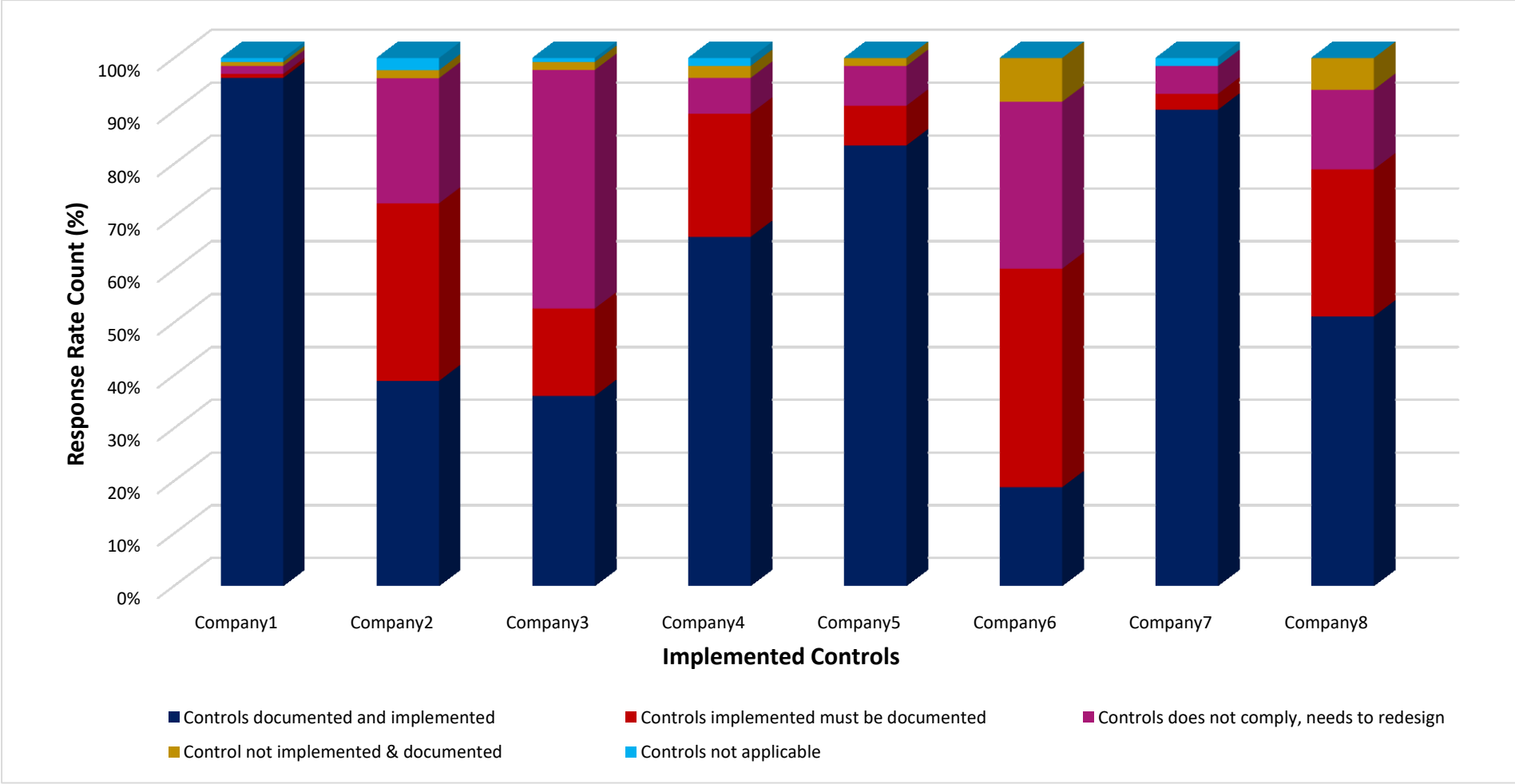


Fig 4.19: Status of implemented Controls

4.4.2.3.3 ICT Security Base Practice Implementation based on ISO27001 Clauses 4 to 10 status

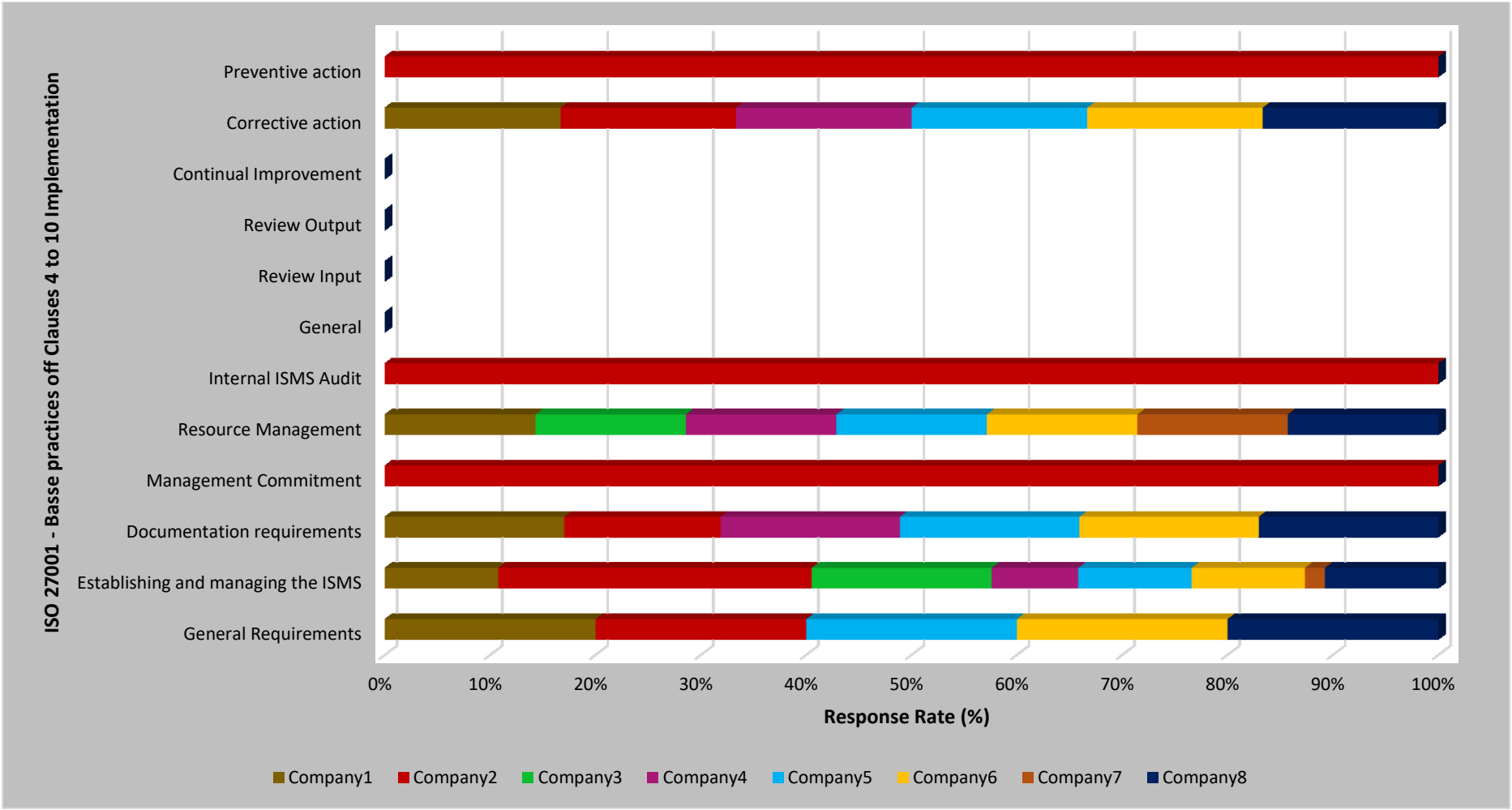


Fig 4.20: ICT security Base practice Implementation based on ISO27001 Clauses 4 to 10 status.

4.4.2.3.4 ICT Security Base Practice Implementation Status based on ISO27001 Annexure a Controls.

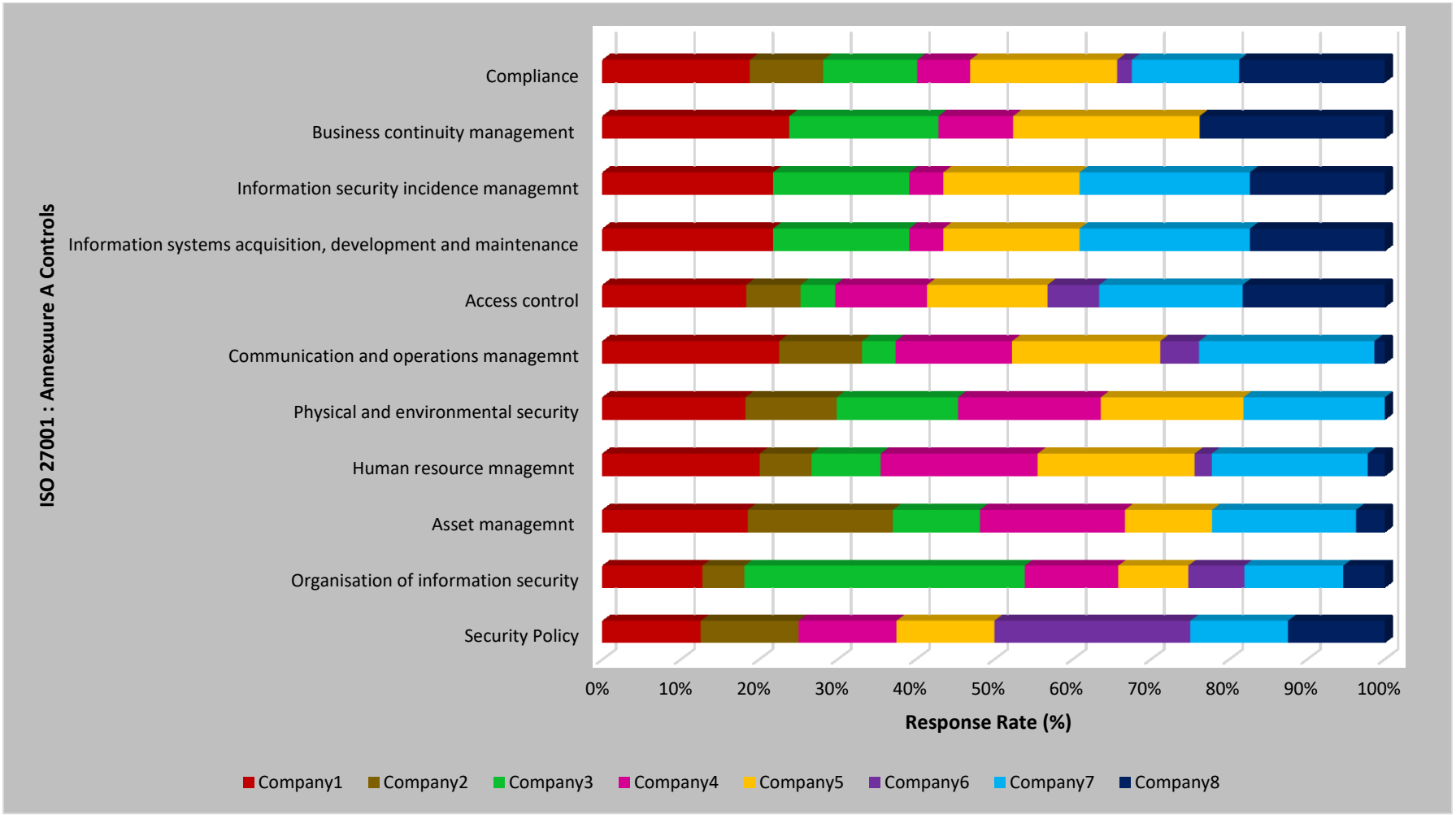


Fig 4.21: ICT security Base practice Implementation Status based on ISO27001 Annexure A Controls.

4.4.2.3.5 Organisational Function Involvement in the management of ICT/Cyber Security.

The findings from the respondents revealed that there is recognition of ICT/Cyber security in some organisations as evidenced by functional involvements shown in Fig 4.22. However, , despite the efforts noted in some of the public organisations that strive to prevent misuse of the financial, personal and confidential information of its clients and employees, the ICT /Cyber Security posture was not convincing, because data is still leaked

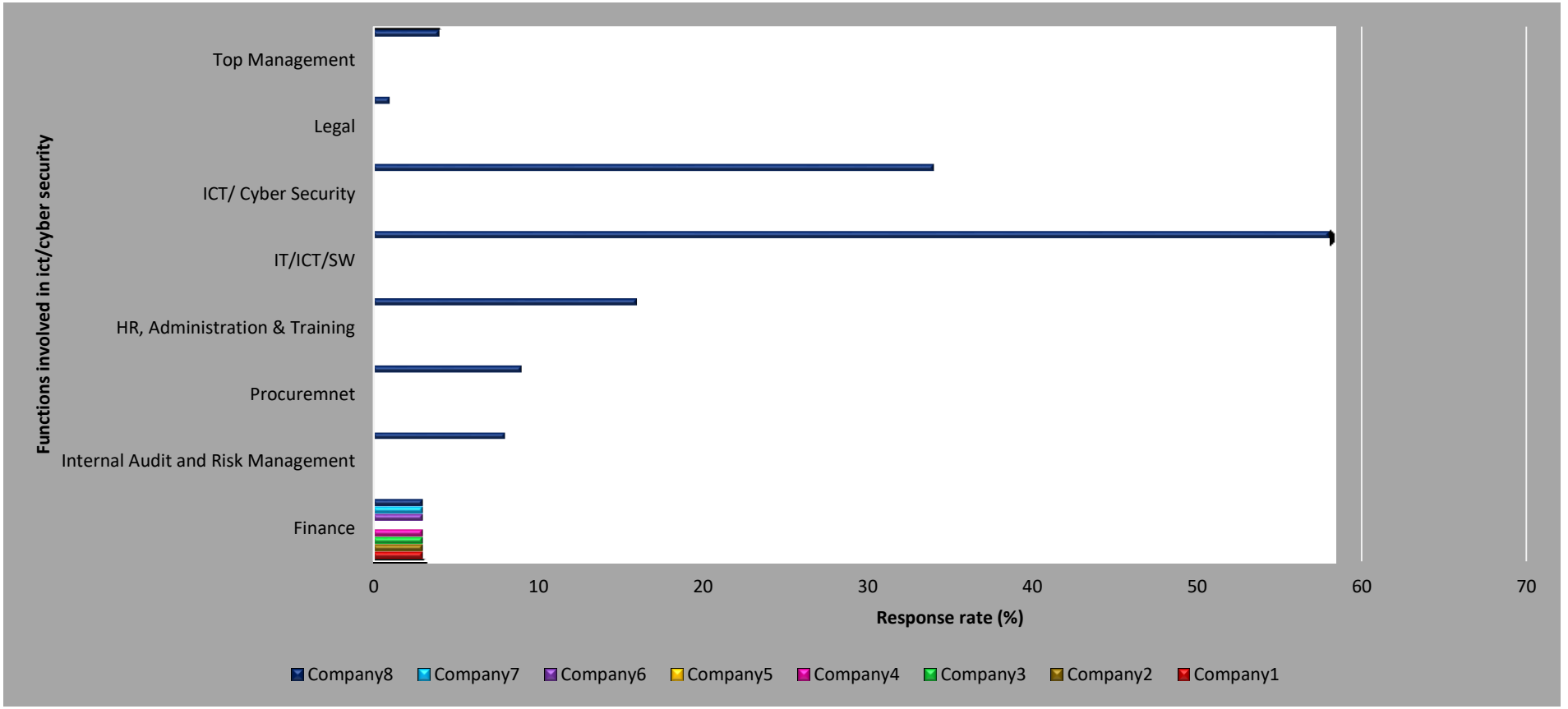


Fig 4.22 Organisational Function Involvement in the management of ICT/Cyber Security.

4.5 Conclusion of the findings

An investigation of the Cyber Security threats by insiders established that the current controls in the most public organisation are not effective enough to mitigate Cyber Security insider threats, with most of them still struggling to establish the departments and workforce for the general ICT/Cyber Security that is also expected to take care of the insider cyber threats.

The research further established that there is luck of Cyber Security awareness and later on preparedness in public organisations which is evidenced by the lack of the National Cyber Security Policy. Most of the employees have very little knowledge of Cyber Security and its effects on their privacy as well as the economic development of Zambia.

4.6 Chapter Summary

This this chapter has presented the findings from the participants during the research fieldwork. The findings are based on management and workers from the eight selected public organisations. The next chapter discusses the findings in detail. It provided the results of the empirical data analysis for the study, as well as data presentation as obtained during data collection. This aimed at fulfilling all the three research objectives which were looking at investigating the public organisations' Cyber Security threats posed by an insider as well as determining the effectiveness of the current controls particularly to do with protection against internal Cyber Security threats.

CHAPTER FIVE

DISCUSSIONS OF RESULTS

5.1 Introduction

This section discusses the relevance of the findings of the research to the objectives of the study and provides answers to the research questions after analysing the results in Chapter 4. This will be achieved through triangulation by linking the various evidence from the secondary research presented in Chapter 2 to the evidence gathered from the primary research and the research questions. It analyses the findings in relation to the existing body of knowledge on the mitigation of cyber threats by organisational insiders. With a high focus on what cause insiders to attack their employers, and what controls are expected to be in place for mitigation in public organisations. The earlier discussion findings with literature were important in determining how this research fits in the body of knowledge on the subject matter. It further provides a basis for comparisons on how the research has contributed to the filling of the previous missing gaps in the body of knowledge. This was carried out in line with the research objectives and the questions.

5.2 Recognition of the need for ICT/Cyber Security departments in Public Organisations

5.2.1 Availability of Cyber/ICT Security departments

The research revealed that despite the fact that 62.5% of the Public organisations under review has established ICT/Cyber Security departments, only 25 % had fully qualified Chief Information Security Officers (CISO) with both professional and academic qualifications. A few traces of security being headed by a university graduate without ICT/Cyber Security background whatsoever or with just several years of experience which amounted to 12.5%. The other 37.5 % of the public organisations had completely not established ICT/Cyber Security departments as indicated in Fig 4.5. However, the organisations had functioning IT departments that is specifically offering IT Service Management ITSM, hardware and networking services. The only security aspect concerned with the IT department was the Endpoint security.

Based on industrial base practices, the public organisations executive management needs to show support and buy-in by establishing the Cyber Security departments with qualified ICT/Cyber Security

staff as well as funding the necessary ICT/Cyber Security initiative considering the fact that embracing technology is one of Zambia's focus area as stated in the Seventh National Development plan (7NDP).

5.2.2 ICT/Cyber Security Staff Establishment

The research revealed that out of the 62.5% of the Public organisations under review that had established ICT/Cyber Security departments, only 25% of the organisations had an average number of established and qualified ICT/Cyber Security staff. These were ranging between six (6) to ten (10) employees despite the fact that they are unable to manage insider threats due to understaffing. Meanwhile, 37.5% had a handful of established and qualifies ICT/Cyber Security employees ranging between one (1) to five (5) members. Just like in the department establishment, the other 37.5 % of the public organisations had completely no established ICT/Cyber Security staff. There was no single organisation that had more than ten (10) ICT/Cyber Security staff. However, through interviews, the research established that of those organisations who have established ICT/Cyber Security staff only about 60% had qualified both professionally and academically ICT/Cyber Security staff as indicated in Fig 4.6. Further, the numbers of established staff are not convincing to manage the traditional infrastructure perimeter security from external hackers as well as the managing insider's threats as an added assignment. This leaves most of the public organisations vulnerable to insider attacks.

After getting management support and buy-in, it's now time for HR to establish the ICT/Cyber Security department as well as qualified staff both academically and professionally. These are required to carry out the day to day running of the department whose objective is to ensure data confidentiality, integrity and availability.

5.2.3 Executive Management's Buy-In and Support for the Cyber/ICT Security Department

The research established that 62.5% of the Public organisations under review had average management buy-in and support for ICT/Cyber Security department and initiative raging between very well and moderately supported, which will later entail management of insider threats. 12.5% of the organisations are very well supported whilst 25% are adequately supported with another 25 % being moderately supported. In the same vein, just like in the department and staff establishment, the other

37.5 % of the public organisations do not have the management buy-in and are not supported indicated in Fig 4.7.

Management is required to demonstrate support and buy-in by approving the ICT/Cyber Security related policies, procedures, standards, initiatives and budget. Without Management support, it is impossible to effectively manage an ICT Security Department and later on ensure data security.

5.2.4 Executive Management's funding of the Cyber/ICT Security Department Projects

The research established that 62.5% of the Public organisations under review was on average, adequately to moderately funded, with just a few traces of poor funding spotted in two (2) organisations from the respondents. In the same vein, just like in the department and staff establishment, as well as the management buy-in and support, the other 37.5 % of the public organisations do not have the managements buy-in and are not funded as indicated in Fig 4.8.

The ICT/Cyber Security department and initiative can have the management's partial support and buy-in, but if there is no adequate compliance and support for funding, the department cannot function because security is quite pricey. This being the simple most reason why management support and buy-in total is important in the management of ICT/Cyber Security department and initiative.

5.2.5 The Percentage ICT Budget Currently Spent On Prevention and Detection of Insider Incidents/Attacks

Statistics from management buy-in, support and Funding above gives an indicator of the possibility for the public organisations to manage insider threats. Majority of the few that approved budgets still were only allowed to spend less than 10% of the ICT budget as indicated in Fig 4.9. Thereby making the management of insider Cyber Security threats a night mere. However, through interviews, the research established that despite some organisations having executive's partial support, the departmental budgets are never approved as per requirement of the department, because management feels its unnecessary cost.

Looking at the cost of implementing international standards and frameworks like COBIT 5.0 and ISO27000, the budgets of less than 5% off the ICT is not enough to suffice for the required Cyber Security management later on the Insider security threats. This is evident that public organisations are

far from Cyber readiness and need to enhance this call that is emphasised even in the Seventh National Development Plan (7NDP). Lack of budget is a serious vulnerability that an insider can exploit and leave the organisational data unsecured. This is because even the issue of employing more qualified staff, implementation of base practice and well as curbing the perpetrators, all borders on the funding through the approved budget.

5.3 Types of Vulnerabilities That an Insider Can Exploit In Public Organisation

In addressing research question one (1), the research findings revealed 24 vulnerabilities common among public organisations that an insider can exploit and breach data security. These included but not limited to;

i. Fraud or abuse
ii. Exposure of confidentiality
iii. Business information leakage
iv. Compromise of Personally Identified Information (PII)
v. Loss of competitive advantage
vi. Sabotage
vii. Intellectual Property (IP) Theft
viii. Compromise of HR information
ix. Lack of clear communication channels
x. Lack of comprehensive access control
xi. Lack of information Classification Policy
xii. Lack of business continuity Plans
xiii. Lack of Exit interviews
xiv. Lack of technology solutions
xv. Lack of budget
xvi. Lack of appropriate Policies, procedures and standards
xvii. Lack of internal qualified and specialized staff
xviii. Lack of ICT/Cyber Security department establishment
xix. Lack of Comprehensive Awareness Plan
xx. Lack of Comprehensive and specialized training

xxi. Technology Complexity

xxii. Lack of administration for insider threats and control

xxiii. Lack of Executive management support and buy-in for ICT/Cyber Security initiative

xxiv. Absence of employee screening and background checks.

The most common nine (9) that rated above 50% according to respondents being Fraud or abuse, exposure of confidentiality, Sabotage, lack of training, lack of policies, procedure and standards, technology complexity, lack of insider threat administration, lack of executive support and compromise of HR information as indicated in Fig 4.10. These are the vulnerabilities that require immediate attention as well as full manage.

5.4 Effectiveness of the Current Controls

In addressing research question two, a number of assessments including control analysis and verification ware carried out.

5.4.1 Insider Attack Experience and the Estimated Cost of Loss Due to Insider Attack

The research established that 75% of the Public organisations under review have averagely experienced insider attacks before. Whilst 25 % were not sure whether they have experienced the insider attacks before or not. However, during the interviews, all the respondents confirmed having had experienced the attacks before but could not publicise due to fear of losing customer confidence. Therefore, they decided to keep the information with the organisation so as not to lose a competitive advantage and reputational risk. This means that insider attacks experience is rated at approximately 100% as indicated in Fig 4.11.

About 50% of the organisations reported having suffered losses amounting to USD ninety-nine thousand ($99,999) in the past revenue due to insider attacks. Other incidences from various organisations amounting to 50% of the organisations have experienced loses amounting between USD hundred thousand ($100,000) and USD two hundred and forty nine thousand ($249, 000). Incidences with revenue losses amounting between USD 2.5 million to USD 5million was experienced by 12.5 % of the organisations whiles the highest loss recorded of above USD 5 million was experienced by

25% of the organisations as indicated in Fig 4.12. During interviews, it was revealed that the recorded costs were just a tip of the iceberg because other loses could not be told.

This is despite the efforts and executive management support in some of the organisations as well us having put in place a few policies, procedures, standards and plan to manage insider threats.

In one of the control questions, the responders confirmed that the controls put in place have not had an impact in the mitigation of the insider threats because there has never been a reduction in the attacks whatsoever. They just keep revolving.

5.4.2 Status of the Administrative Policies & Procedures

Administrative policies & procedures used in preventing, detecting and mitigating actual insider threats incident or attack per company. The research findings as indicated in Fig 4.13, revealed that all the public organisations under reveal have at least implemented more than 50% of the insider threat administrative policies and procedures as listed below;

i. ICT Security Policy & Procedures
ii. Comprehensive NDA Policy
iii. Employee screening Policy
iv. Exit Policy /Procedure
v. Clear Desk Policy
vi. None of the above
vii. Awareness Policy & Procedures
viii. Information Classification Policy
ix. Role-based access control policy
x. Acceptable use policy
xi. Access Control Policy

However, it was revealed during interviews that these policies and procedure are only known to the developers and some they have never even reviewed then whilst others are in draft format and have never been approved for ages. The effectiveness of a policy and procedure can only be measured through enforcement and awareness with users' acknowledgement of having read and understood the

policy or procedure as well as having attended an awareness session and comprehended the content. This is because the users are the role players who are expected to comply with the policies and procedures in mitigating insider threats.

5.4.3 Mandatory Screening and Underground Check For Prospective Employees

ICT /Cyber Security and HR departments should carry out mandatory screening and underground check for prospective employees before they are employed.

The research revealed that only 25% of the Public organisations under review have on average policy to undertake mandatory screening and underground check for prospective employees before they are employed. 12.5% was partially adopted whilst 62.5 % have neither implemented nor adopted the mandatory screening and underground check for prospective employees before employing them as indicated in Fig 4.14.

This poses a high risk as organisations as they may be rotating the same perpetrators who have been fired from one organisation to the other. It is a base practice to adopt mandatory screening and underground check for prospective employees for all public organisations.

5.4.4 Exit Interviews

Organisation that mandate exit interviews before paying off the benefits of any leaving employees or contractors. The research revealed that only 25% of the public organisations under review have on average policy to mandate exit interviews before paying off the benefits of any leaving employees or contractors. 25% were not sure whilst 62.5 % have neither implemented nor adopted the mandatory exit interviews before paying off the benefits of any leaving employees or contractors.

At the leavers, the interview is when the contractor and employee are reminded of the DNA signed at the begging of the contract and asked to sign for reassurance of having understood the contents of the policy as well as the consequences punitive actions that can be taken against them should they decide to divulge corporate classified information.

It is a base practice to mandate exit interviews before paying of the benefits of any leaving employees or contractors for all public organisations.

5.4.5 Mandatory Non-Disclosure Agreement (NDA) Policy with Deliberate Clauses

An organisation that has a mandatory Non-Disclosure Agreement (NDA) Policy with deliberate clauses to deter the exiting employees or contractors from leaking the organisational information and sabotaging the organisation. The research established that only 50% of the public organisations under review have on average in place, NDA policy with deliberate clauses to deter the exiting employees or contractors from leaking the organisational information and sabotaging the organisation. The other 50 % have do not have the NDA policy in place. However, during interviews, it was discovered that only 37.5% have recorded an above average compliance to the policy as indicated in Fig 4.15. Leaving 62.5% which is the majority without implementing and enforcing compliance with the NDA policy.

This is a critical vulnerability that an insider can exploit into a high risk to organisational insiders as they are aware that they have never signed any legal binding document to deter them from leaking any type of information to the outsiders. It is a base practice to adopt and implement a mandatory NDA policy for all public organisations.

5.4.6 System Access Control Policy

Access control policy for user access rights deactivation after termination of the contract. The research established that only 62.5% of the public organisations under review disable user access rights and access cards to the premises immediately after termination whilst 25% disable after a couple of hours and 12.5% disables after a day.

However, during interviews, it was discovered that some organisations from the 62.5% category above take as long as a 1 month to a year with past user access still active. This is more so especially for the senior and executive management as well as the role players with whom it takes time for HR to inform the ICT or Security department to disable users. Some examples included employees who have been transferred from one department to other, promoted demoted who still maintain the access rights they have had from their previous roles.

This is yet another critical vulnerability that an insider can exploit and cause a high risk to organisational data which is supposed to be protected from leaking and ending up in the hands of the

unauthorised. It is a base practice to adopt and implement a role-based access control for all public organisations in an endeavour to mitigate insider cyber threats.

5.4.7 Incident Response Plans' Special Provisions for Insider Related Incidents

The research established that only 12.5% of the public organisations under review have a formal incident response plan with special provision for insider related incidences, whilst 50% have no formal incident response plan with special provision for insider related incidences. 37.5 % were not sure.

However, during interviews, it was revealed that over 75% of the organisations have no incident response plan with special provision for insider related incidences in place as indicated in Fig 4.16.

Just like in the other discussed vulnerabilities, lack of a formal incident response plan with special provision for insider related incidences is another critical vulnerability that an insider can exploit and cause a high risk to organisational data which is supposed to be protected from leaking. It is also difficult for the security personnel to learn from the previous insider incidences, to ensure business continuity. CISO's need to keep a record of all insider related incidences so as to ensure they prevent the same from re-occurring. This can only be achieved if the insider incidences are part of the incident response plan. It is a base practice to include insider threats in the formal incident response plan with for all public organisations in an endeavour to learn from the past incidences and mitigate insider cyber threats.

5.4.8 Effectiveness of the Current Controls in addressing Insider Threats

The findings above revealed that the current controls in place are not effective enough to mitigate threats to an acceptable level. While 62.5% of the respondents from the public organisations under review confirmed that their controls are not effective as indicated in Fig 4.17, all the organisations have continuously experienced insider attacks with huge revenue losses. The control questions during the interview actually reviewed and confirmed that there is a need to readdress the all the controls in place if insider threats are to be mitigated to an acceptable level. More than 50% of public organisations investigated, only had partial ICT security-related policies and procedures in place. Nonetheless, the documents are not known to the role players who are in turn expected to comply in

order to ensure data security. Meanwhile, about 25% of the organisations were found to not have an ICT/Cyber Security department or ICT/Cyber Security specialized staff to effect the security controls.

5.5 ICT/Cyber Security GAP Analysis

In addressing research question 3, a gap analysis based on ISO 27001:2013 standard was carried out establish the gaps in the current ICT Security controls so as to be able to possibly recommend mitigating measures to insider threats that will be in tandem to the International standard ISO 27001:2013 that can address the issues in question (i) and (ii) above.

5.5.1 ICT Security Process Implementation

The findings revealed that Gap analysis of the public organisations under review based on the current status of Information Security base practice adoption of the organisations as per ISO 27001:2013, compliance levels were below 30% as indicated in Fig 4.18.

Overall, all the assessed organisations' results were below the average of the standard compliance measure of 100. The current status poses a serious vulnerability to the organisations' information which is supposed to be protected.

5.5.2 ICT Security Base Practice Implementation based on ISO27001 Clauses 4 to 10

The findings revealed that Gap analysis of the public organisations under review based on the ISO 27001 Clause 4 to 10 that includes;

4. Organization Context
5. Leadership
6. Planning
7. Support
8. Operation
9. Performance evaluation
10. Improvement.

All the assessed organisations' results were below the average of the standard measure as indicated in Fig 4.20. The current status poses a serious vulnerability of the organisations' information and requires an immediate attention.

5.5.3 ICT Security Base Practice Adoption based on ISO27001 Annexure A Controls

The findings revealed that Gap analysis of the public organisations under review based on the baseline assessment for security maturity level based on ISO 27001: Information Security Management System (ISMS) Annex A domains that include;

i. A.5 Information security policies
ii. A.6 Organization of information security
iii. A.7 Human resource security
iv. A.8 Asset management
v. A.9 Access control
vi. A.10 Cryptography
vii. A.11 Physical and environmental security
viii. A.12 Operations security
ix. A.13 Communications security
x. A.14 System acquisition, development and maintenance
xi. A.15 Supplier relationships
xii. A.16 Information security incident management
xiii. A.17 Information security aspects of business continuity management
xiv. A.18 Compliance.

Overall, all the assessed organisations' results of the security controls implemented were below the average of the standard compliance measure of 100% as indicated in Fig 4.21. The current status poses a serious vulnerability to the organisations' information which is supposed to be protected.

The assessed organisations have knowledge of the importance of securing organizational data. They all have the Cyber/ICT Security Policies that aligns with the organization's corporate objectives and also defines security measures. However, these organisations need improvement based on the basic required documents of the security departments to address the mitigation of insider threats [5]. These

are mandatory documents for a cyber-ready organization in combating insider threats including; Cyber/ICT security policies, strategy, business continuity policies, classification of information procedure, classification of assets procedure, incidence handling procedure, pre-employment screening policies, Leavers interview policies, Comprehensive Non-disclosure agreements, Clear desk clear screen policies, Mobile device management policies and information handling and transfer policies, user awareness policies among others.

The assessed organisations are also cognizant of the international ICT security standards and have since adopted a number among them being ISO 27001:Information Security Management System (ISMS), ISO 9001: Quality Management System (QMS) and ISO 33001 Risk Management System(ERM), Control Objective for Information and Related Technologies (COBIT) 5.0, ITIL among others. However, compliance has proved to not be adhered too. There is a need for enhancements together with consistency in order to address insider threats. The adopted standards necessitate some policies, procedures, guidelinesand processes to be formulated, approved and distributed to the users so as to ensure compliance which initially has not been the case at the time of this study.

During the baseline assessment, it was evidenced that the access control policies are not fully implemented and enforced for compliance purposes, this leaves a doorway to malicious insiders by leaving valuable information susceptible to attacks. This, in turn, makes the entire infrastructure vulnerable as insiders are able to explore the ANT and TPB for their planned attacks.

There is no proper alignment of information security and ICT risk management, leaving ICT Risk management unclear to the stakeholders. No Risk plan, neither risk registers nor risk treatment plans are in place. All these vulnerabilities point to insider threats.

Information security effectiveness and performance requires an evaluation and redesign of an ISMS as so as to comply with the adopted standards and frameworks.

Some organisations have approved information security policies, but the procedures are not in place. ICT/Cyber Security objective has been developed but no Key performance indicator (KPI’s).

The few organisations that had adopted the ISO 27001 and or COBIT 5.0, lacked enforcement and incorporation of information security controls as required by ISO 27001:2013 in various processes which includes architecture, incident management, change management, operations, access management, business continuity, human resource, physical security, asset management and project management.

The evaluation of information security performance and the effectiveness of the information security management system are not clearly documented or being performed. The Company 1's current ICT security product portfolio covers the minimal ISO 27001:2013 requirements and need to be reviewed.

These assessments identified gaps in the existing organization ISMS which all points to the fact that they are operating in a vulnerable environment to insider threats. The perpetrators may leverage on the adverse effect of ANT and the TPB leading to Insider Crimes.

The above are the identified gaps in the existing policies, procedures and processes in the management of ICT security in the organisation leaving it vulnerable to the negative impact of ANT and the TPB that leads to Insider Crimes. They provided evidence despite the organization's effort on combating external attacks, the enemy is just within. The systems are not secure enough to defend from insider threats. Notwithstanding the element of the organisations' effort of securing critical data, the environment is vulnerable and requires urgent attention. There is a need for extensive awareness so that, as the corporations budgets for systems and put security tools in place, users should be made aware so they can help with the prevention and detection of the vulnerabilities.

5.6 Proposed Mitigating and Countermeasures

Based on the results, we wish to propose a model of minimum insider mitigation instruments, with the behaviour factor addressed in question 1. The proposed model aligns with ISO 27001 and COBIT 5.0 security requirements, such that should an organisation decide to implement the international standards, they will not have to reinvent the wheel. The proposed model is cheap and sustainable for the environment considering the high costs of implementing international standards which is currently a deterring factor. It adds to the body of knowledge. The steps of measures must be considered in order to avert the insider threat with the top being user awareness. They are further presented in a model as in Fig 5.1.

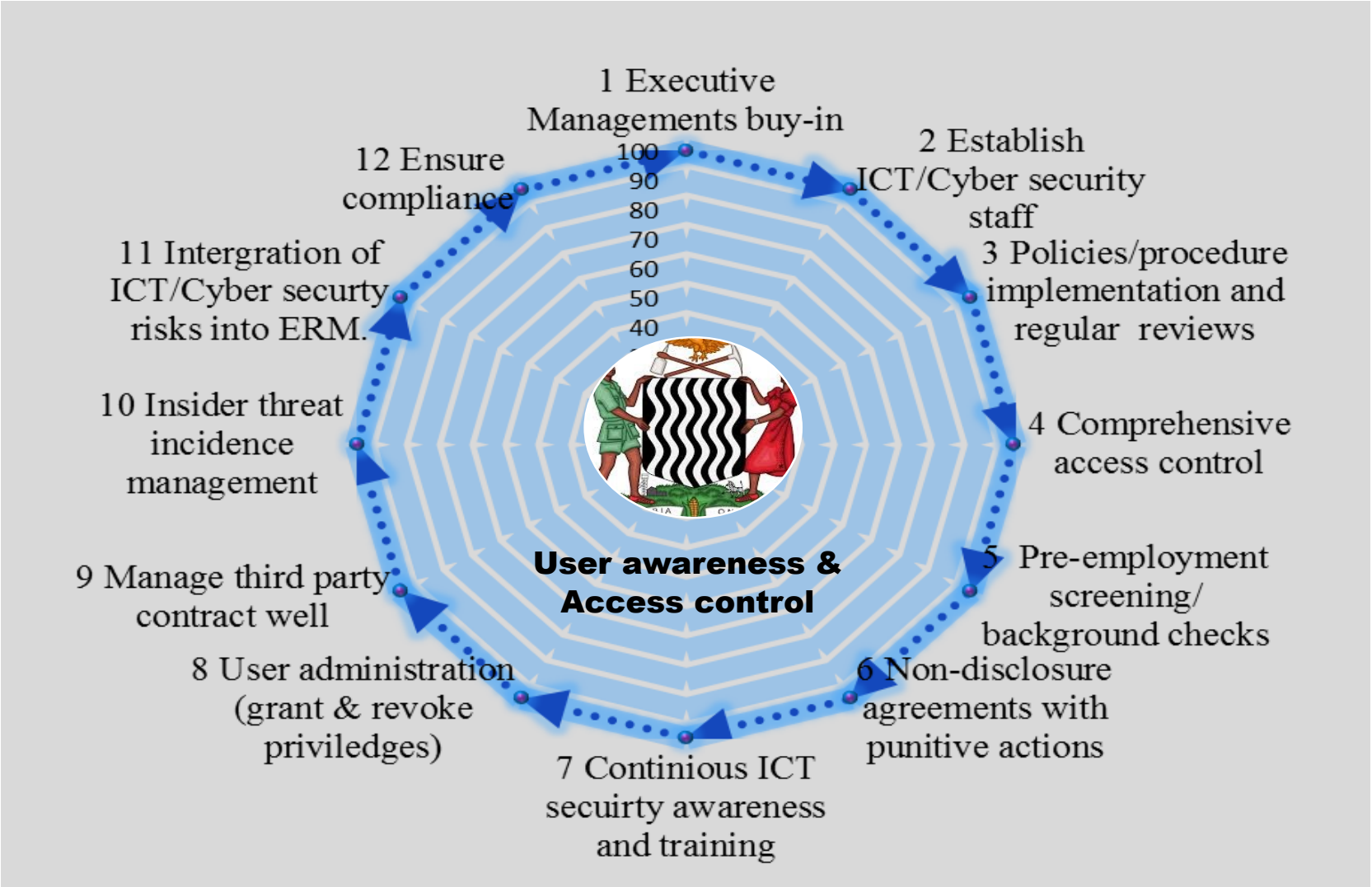


Fig 5.1: Proposed Insider Mitigation Model with Minimum Instruments

1) **Executive Management Buy-In: Management Is Required to Demonstrate Support and Buy-In** by approving the ICT/Cyber Security related policies, procedures, standards, initiatives and budget. Without Management support, it is impossible to effectively manage an ICT Security Department and later on ensure data security. This is priority number one in managing data security.

2) **Establish ICT/Cyber Security Department and Staff:** After getting management support and buy-in, it's now time for HR to establish the ICT/Cyber Security department as well as qualified staff both academically and professionally. These are required to carry out the day to day running of the department whose objective is to ensure data confidentiality, integrity and availability.

3) **Relevant Administrative Policies and Procedure Implementation and Regular Reviews:** When the department, as well as the required and qualified staff, are established, it's not time to formulate policies and procedures, implement and enforce them to ensure compliance.

4) **Comprehensive Access Control:** It is required to manage all access to both the systems as well as the premises. They must be well structured and monitored with automated rules, and for system access, users must be well trained and aware, access should be Role Based and strictly monitored.

5) **Pre-Employment Screening:** Organisations must adopt mandatory screening and underground check for prospective employees before employing them. This is so, to prevent organisations from rotating the same perpetrators who have been fired from one organisation to the other, as well as those who are naturally known to be bad guys. This necessitates the maintenance of the integrity and confidentiality of organisational data, the rule must apply to both employees and externally hired personnel. The prospect employees must if possible present a certificate of good conduct.

6) **Non- Disclosure Agreements with Spelt Punitive Actions:** Employees must sign a secrecy agreement known as a Non- Disclosure Agreements (NDA) with well-spelt consequences of being found to guilty of a malicious insider. The punitive actions must be very grave enough

to deter users from engaging in insider crimes, and users must be made aware on a continuous basis. All contracts for employees, contractors or any business associates must contain paragraphs that cover non-disclosure-requirements, non-compete requirements or other statements on the confidentiality and integrity of the information that the organisation processes and users must be made aware on a continuous basis.

7) **Continuous ICT Security Education and Awareness:** Employees and contractors or any business associates must be informed about the rules of ICT/Cyber Security and integrity at entry into the their roles and on a continuous basis through trainings (online and face to face) broadcasted security tips as well as availability of all relevant documents in a central repository that describes the rules for Information Security, and guidelines that users must be made aware on a continuous basis.

8) **User Administration / Revocation of Authorizations:** There must be a checklist for functional changes and retirement of personnel. Logical and physical authorizations are withdrawn at the latest on the last working day and hour. This is more so especially for the senior and executive management as well as the role players with whom it takes time for HR to inform the ICT/Cyber Security department to disable users. Some examples included employees who have been transferred from one department to other, promoted demoted who still maintain the access rights they have had from their previous roles.

9) **Third Party Contracts:** In case of outsourcing the services or activities, there is a need for the suppliers and or contractors to be inducted and made aware of the organisational policies so as to comply with the stated procedures for data security purposes.

10) **Insider Threat Incidence Management:** ICT security incidents must be registered, analysed, watched over and reported to the persons in charge as stated the security incident guideline and users must be made aware on a continuous basis. This is so as to ensure security personnel can learn from the previous insider incidences, to ensure business continuity. CISO's need to keep a record of all insider related incidences so as to ensure they prevent the same from re-occurring. This can only be achieved if the insider incidences are part of the incident response plan.

11) **Integration of ICT/Cyber Security Risks into Enterprise Risk Management (ERM):** ICT/Cyber Security risks are very critical to the success of the organisational operations. It is therefore imperative that they must be integrated into the Enterprise Risk Management (ERM) so that they are looked at from an entire organisational point of view.

12) **Manage Compliance:** ICT/Cyber Security Compliance incorporates all business functions in organisations, therefore, it calls for combined and considered efforts from all organisational stakeholders. This involves adhering to a wide range of laws, standards, frameworks, policies and procedures which are designed to protect the organisation employees and other stakeholders. Because of the vast number of guidelines for compliance, it can be easy to be in violation, leaving organisations open to penalties and even dissolution. Therefore, having a complete and thorough understanding of ICT laws, standards, frameworks, policies and procedures is crucial to protecting organisations in the years to come.

5.7 Chapter Summary

This chapter discussed and analysed the findings of chapter four in details as they relate to the objectives in relation to the existing body of knowledge on the subject matter of Insider Cyber threats in public organisations.

CHAPTER SIX

CONCLUSION AND RECOMMENDATIONS

6.1 Introduction

This chapter essentially gives the conclusion and recommendation of the study. The previous chapters have expanded on the importance and need of investigating into Cyber Security threats by posed by organisational insiders in Zambia's public organisations. Various literature sources were reviewed with a high focus on the challenges of mitigating insider threats. From the research findings, the researcher, directed by the objectives of the study, concludes and recommends the following for the purposes of the Cyber Security preparedness to enhance data security in Zambia.

6.2 Chapter Summary

The overall aim of the study was to investigate into Cyber Security threats posed by insiders and enhance insider threat mitigation controls in public organisations focusing on the challenges and solutions thereby securing critical data. The research objectives were provided in Chapter one which indicated that the literature would be reviewed, followed by data collection, analysis findings and discussions. The research synopsis was repeated in this section.

Chapter Two looked at the background literature and the related studies which meet the objectives by comparing and contrasting the previous works of other researchers and provide support for the development of a proposed Insider cyber threat mitigation model to reduce the risks associated with insider threats to an acceptable level. It discussed a number of factors affecting insider security management in public organisations. It highlighted the meaning of ICT/Cyber Security culture in organisations, the various indicators to ICT/Cyber Security and how they can be related to the public organisations. Numerous challenges were identified from the various literature reviewed. The ultimate conclusion of the chapter from the literature reviewed indicated the gaps in the factors and challenges to organisational ICT/Cyber Security culture.

In Chapter Three, the research approach was outlined in which the method and procedures for administering the questionnaires, data collection and analysis was also discussed including statistical

methods namely descriptive statistics. It further discussed the sample size, sampling processes as well as the justifications which were employed before considering the data collection approach, instruments, methodological reliability and validity of various techniques used in this study.

Chapter Four provided the results of the empirical data analysis for the study, as well as data presentation as obtained during data collection. This aimed at fulfilling all the three research objectives which were looking at investigating the public organisations' Cyber Security threats posed by an insider as well as determining the effectiveness of the current controls particularly to do with protection against internal Cyber Security threats.

Chapter five discussed and analysed the findings of chapter four in details as they relate to the objectives in relation to the existing body of knowledge on the subject matter of Insider Cyber threats in public organisations.

Finally, the last chapter provides the conclusion and recommendation based on the findings and analysis of the research based on the literature review, findings and analysis in line with the objectives and research questions for future studies in the same area.

6.3 Review of Research Objectives

6.3.1 First Objective

To establish the types of vulnerabilities in public organisations that can be exploited by insiders. This objective was achieved and the study findings have established that there are vulnerabilities that can easily be exploited by an insider thereby cause data security breach in public organisations. The identified vulnerabilities showed clear linkages of organisational ICT/Cyber Security culture based on the research questions. The factors delineated from the study that can be used in effecting a positive organisational ICT/Cyber Security culture and they include:

- Executive management support and support
- Continuous improvement of ICT/Cyber Security policy and procedure reviews
- Continuous improvement awareness and training through Corporation values, stakeholder involvement

- Improved Communication channels
- ICT/Cyber Security risk management
- Compliance Management.

6.3.2 Second Objective

To establish the effectiveness of the current controls in public organisations in protecting against potential Cyber Security threats from insiders. This objective was achieved and the study findings established that the current controls in place are not effective enough to mitigate threats to an acceptable level. This is due to the fact that, all the organisations have continuously experienced insider attacks with huge revenue losses despite having the controls in place. Majority of the public organisations investigated only had partial ICT security-related policies and procedures in place. Nonetheless, the documents are not known to the role players who are in turn expected to comply in order to ensure data security. Meanwhile, about 25% of the organisations were found to not have an established ICT/Cyber Security department or ICT/Cyber Security specialized staff in place to effect the security controls.

6.3.3 Third objective

To propose measures to mitigate insider threats. This objective was achieved and based on the findings, we wish to propose a model of minimum insider mitigation instruments, with the behaviour factor addressed in question 1. The proposed model aligns with ISO 27001 and COBIT 5.0 security requirements, such that should an organisation decide to implement the international standards, they will not have to reinvent the wheel. The proposed model is cheap and sustainable for the environment considering the high costs of implementing international standards which is currently a deterring factor. It adds to the body of knowledge. The steps of measures must be considered in order to avert the insider threat with the top being user awareness. These are presented in a model as in Fig 5.1.

6.4 Research Conclusion

The study has provided useful information involving ICT/Cyber Security mitigation in public organisations in Zambia. Having developed a literature base from related works done from other countries. A questionnaire survey and interviews were conducted with performed statistical analysis to arrive at the useful information for both the study and the body of knowledge.

ICT/Cyber Security departmental and qualified staff establishment is key in the management of insider threats, 62.5% of the Public organisations under review has established ICT/Cyber Security departments, with only 25 % that had fully qualified Chief Information Security Officers (CISO) with both professional and academic qualifications.

Cyber Security Vulnerability assessment is key to management of insider threats and Cyber Security as a whole. The assessment conducted during the research reviewed a number of vulnerabilities that can easily be exploited by the perpetrators which can leave the organisational data un-secure.

ICT/Cyber Security policies and controls are required to be aligned to the organisations' strategic objectives so as to enhance controls effectiveness and easy of performance measurement in relation to key performance indications (KPI) and compliance. Public Organisation needs to consider minimum mitigation measures for insider threats in as a step in the cyber readiness direction, looking at the difficulty of modelling human behavior.

The study made a significant contribution to ICT/Cyber Security management through knowledge on the existence of challenges to organisational ICT/Cyber Security culture with respect to insider threats. The major challenges highlighted by the research are management to buy-in and support the ICT/Cyber Security initiatives because it is perceived as unnecessary expense considering the high cost of implementing ISMS.

Finally, the achievement of best practice of organisational ICT/Cyber Security culture will go a long way in helping to model human behavior which is key to the management of insider threats. Up until now, the findings from both the secondary and primary research undertaken have shown a thorough exploration of the research subject and reasonable conclusions have been made. It is the belief of the researcher that the evidence revealed in this work have shown a significant picture of the ICT/Cyber

Security readiness and security posture of Zambia as a nation. Therefore, the overall aim which was to enhance insider threat mitigation controls in public organisations focusing on the challenges and solutions thereby securing critical data of the research was achieved.

6.5 Recommendations

The author recommends that Public organisations Executive Management should;

- Adopt the proposed model as a minimum requirement for the mitigation of Cyber Security threat by organisational insiders
- Commit support to ICT/Cyber Security management by approving ICT and ICT security-related policies and procedures implementation and compliance on regular reviews
- Ensure that ICT risks are integrated into the organisational Enterprise Risk Management (ERM) program.
- Ensure ICT security is included in all ICT related projects and developments for security compliance purposes
- Consider adopting an international standard and framework like ISO27001 or COBIT 5 for security
- And lastly, Government should consider implementing a national Cyber Security policy and passing a penal law to prosecute insider attackers.

6.6 Chapter Summary

This chapter provided the conclusion and recommendation based on the findings and analysis of the research based on the literature review, findings and analysis in line with the objectives and research questions for future studies in the same area.

REFERENCES

[1] Melissa K. Chinyemba and Jackson Phiri, - An Investigation into Information Security Threats from Insiders and how to mitigate them: A Case Study of Zambian Public Sector. Journal of computer science, DOI : 10.3844/jcssp.2018.1389.1400. Available at: https://thescipub.com/abstract/10.3844/jcssp.2018.1389.1400

[2] CHINYEMBA, Melissa K.; PHIRI, Jackson. - Gaps in the Management and Use of Biometric Data: A Case of Zambian Public and Private Institutions. Zambia ICT Journal, [S.l.], v. 2, n. 1, p. 35-43, june 2018. ISSN 2616-2156. doi: https://doi.org/10.33260/zictjournal.v2i1.49

[3] Lubasi Musambo & Melissa K. Chinyemba, Identifying Botnets - 2017. IEEE – 2017 International Conference in Information and Communication Technologies (ICICT). Lusaka, IEEE - Zambia Section.

[4] Report Of The Public Accounts Committee - Parastatals Bodies And Other Statutory Institutions For The Financial Year Ended 31st December, 2014 For The Fifth Session Of The Eleventh National Assembly Appointed By The Resolution Of The House On Friday, 25th September, 2015. (P. 116 - 118) Sourced From: http://www.parliament.gov.zm/sites/default/files/documents/committee_reports/Report%20of%20the%20Public%20Accounts%20Committee%20-%20Parastatals.pdf - Accessed on 01/05/2017.

[5] COBIT 5 for security - www.isaca.org/COBIT-5-for-information-security-introduction.pdf, Accessed on 15/02/2018.

[6] Report– Full I.T Internal Audit (General, Application And Infrastructure), of the Public Accounts Committee - Parastatal Bodies And Other Statutory Institutions For The Financial Year Ended 31st December, 2014 For The Fifth Session Of The Eleventh National Assembly Appointed By The Resolution Of The House On Friday, 25th September, 2015. (P. 116 - 118) Sourced: Dec 2016 From: http://www.parliament.gov.zm/sites/default/files/documents/committee_reports/Report%20of%20the%20Public%20Accounts%20Committee%20-%20Parastatals.pdf, Accessed on 15/02/2018.

[7] Common Sense Guide to Mitigating Insider Threats 4th Edition / December 2012 Technical Report/CMU/SEI-2012-TR-012 / CERT Division of the Software Engineering Institute at Carnegie Mellon University.

[8] Nikolaos Pitropakis, Detecting Malicious Insider Threat in Cloud Computing Environments Ph.D. Thesis 2015.

[9] CERT, Unintentional Insider Threats: A Foundational Study. CERT Co-ordination Centre/SEI, Pittsburgh, 2013. Online http://www.sei.cmu.edu/reports/13tn022.pdf, Accessed on 11/07/2017.

[10] Centre for the Protection of National Infrastructure (CPNI), managing the insider threat. CPNI. London, Security Industry Authority (SIA), 2013. EY 2016 Global Forensic Data Analytics Survey.

[11] Chinyemba, M K. & Phiri, J., 2018. ZAPUC – International Conference Paper. Available at :http://icict.org.zm/conferences/index.php/2018ZAPUC/18/paper/view/32

[12] Dempsey, K. Chawla, N., Johnson, A., Johnston, R., Jones, A., Orebaugh, A., Scholl, M., & Stine, K, Information security continuous monitoring (ISCM) for federal information systems and organisations. (NIST SP800–137) Gaithersburg, MD: National Institute of Standards and Technology, September 2011.

[13] Target Data Breach for spilled information report online https://www.forbes.com/sites/maggiemcgrath/2014/01/10/target-data-breach-spilled-info-on-as-many-as-70-million-customers/#2013767ee795, Accessed on 11/11/2017.

[14] Jacinda L. Wunderlich - Thesis -The Insider Threat, Fall 2011.

[15] J. Hunker Associates LLC & Christian W. Probst, Insiders and Insider Threats - An Overview of Definitions and Mitigation Techniques.

[16] Verizon 2016 Data Breach Investigations Report online http://www.verizonenterprise.com/verizoninsights-lab/dbir/2016/?utm_source=pr&utm_medium=pr&utm_campaign=dbir2016), Accessed on 24/10/2017.

[17] ISO 27001:2013 Information Security Management Systems (ISMS) standard – Online www.iso27001security.com/html/27001.html, Accessed on 14/02/2018.

[18] Forrester's Global Business Technographics Security Survey report, 2015.

[19] Volumetric Insider Threat report. March 19, 2015. Online http://www.vormetric.com/campaigns/insiderthreat/2015/, Accessed on 22/09/2017.

[20] Samaneh Tajalizadehkhoob- Online Banking Fraud Mitigation,-Thesis - August 2013.

[21] Christopher J. Callahan September - Thesis -Security Information And Event Management Tools And Insider Threat Detection 2013

[22] The guardian report on Bradley Manning's court case for classified data leakage. online https://www.theguardian.com/world/2013/aug/21/bradley-manning-35-years-prison-wikileaks-sentence, Accessed on 22/09/2017

[23] R. Trzeciak, Insider Threat, the CERT Insider Threat Database, CERT Coordination Centre/SEI, 2011. Online http://www.cert.org/insider_threat/2011/08/the_cert_insider_threat_database.html , Accessed on 27/09/2017.

[24] Cappelli, D., Moore, A., Trzeciak, R., & Shimeall, T. J. Common sense guide to prevention and detection of insider threats 3rd edition – version 3.1. CMU SEI, 2009.

[25] Secretary of the, DON personnel security program (SECNAV M-5510.30). Washington, DC: N09N2 Navy June 2006.

[26] M.R. Randazzo, M. Keeney E. Kowalski, D. Cappelli & A. Moore - Technical Report CMU Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector – 2012.

[27] Microsoft Vulnerabilities Study Report by Avecto: Mitigating risk by removing user privileges 2016 online, http://technet.microsoft.com/en-us/security/dn481339 , Accessed on 20/11/2017.

[28] PWC & Info Security Europe - Information Security Breaches Survey 2015.

[29] https://www.forbes.com/sites/maggiemcgrath/2014/01/10/target-data-breach-spilled-info-on-as-many-as-70-million-customers/#2013767ee795, Accessed on 11/11/2017.

[30] https://hbr.org/2014/09/the-danger-from-within, Accessed on 10/11/2017.

[31] National Cyber Security Penal Law status - http://www.parliament.gov.zm/node/6419, Accessed on 05/04/18.

[32] Collins Chinyama Kachaka's PHD thesis, an investigation into factors determining Cyber Security preparedness in Zambian commercial banks 2016.

[33] Employees as a weakest link in security – IDIOM online https://writingexplained.org/idiom-dictionary/a-chain-is-as-strong-as-its-weakest-link, Access on 10/11/2017.

[34] S. Organisation, "insider-threats-fast-directed-response-37447," in san reading-room, whitepapers Accessed on 11/11/2017, USA.

[35] Federal Standard 1037C – Glossary of telecommunication terms http://thehowlandcompany.com/pdf/fed-std-1037c.pdf, Accessed on 11/11/2017.

[36] Secretary of the, DON personnel security program (SECNAV M-5510.30). Washington, DC: N09N2 Navy June 2006.

[37] https://www.sans.org/reading-room/whitepapers/analyst/insider-threats-fast-directed-response-37447, Accessed on 11/11/2017.

[38] Managing Insider Threat, Ernest and Yung online and available from https://www.ey.com/Publication/vwLUAssets/EY-managing-insider-threat-a-holistic-approach-to-dealing-with-risk-from-within/$FILE/EY-managing-insider-threat.pdf, Accessed on 02/12/2017.

[39] https://csrc.nist.gov/CSRC/media/Presentations/Mitigating-the-Insider-Threat-Building-a-Secure/images-media/fissea-conference-2012_mahoutchian-and-gelles.pdf, Accessed on 02/12/2017.

[40] https://www.fireeye.com/blog/executive- perspective/2016/05/detecting_and_preven.html.

[41] https://www.sagedatasecurity.com/blog/how-to-detect-and-respond-to-insider-threats.

[42] https://www.csoonline.com/article/3239070/risk-management/reading-between-the-lines-the-real-impact-of-insider-threat.html.

[43] Marisa R., Michelle K., Eileen K., Cappelli D. and Andrew M.: Illicit Cyber Activity in the Banking and Finance Sector, TECHNICAL REPORT CMU/SEI-2004-TR-021 ESC-TR-2004-021, 2005. Online available on https://resources.sei.cmu.edu/asset_files/TechnicalReport/2005_005_001_14420.pdf, Accessed on 02/12/2017.

[44] Jason Anthony Smith, Mitigating the cyber threat, Technical Report, RHUL–ISG–2015–12 (RHUL–MA–2015–12).

[45] Michael Juma Abuli, A Framework for Assessing the Insider Threat in Parastatals in Kenya-November, Thesis 2016.

[46] Terje Benjaminsen, The Norwegian Downsizing Approach in Terms of the Insider Threat-An interpretive study, Thesis 2017.

[47] Wesley Cornelissen, Investigating Insider Threats: Problems and Solutions, Thesis, 2009.

[48] Zulkefli Mohd Yusopa and Jemal Abawajy, Analysis of Insiders Attack Mitigation Strategies, elsevier, Journal, Procedia - Social and Behavioural Sciences 129 (2014) 581 – 591 ISSN 1877-0428.

[49] Nec, 2017. Nec Cloud Storage. Online Available at: www.nec.com, Accessed 08/01/2018.

[50] Anil K. Jain and Ajay Kumar Biometric Recognition: An Overview - Michigan State University, East Lansing , MI 48824-1226 , USA.

[51] Yu Cai, E. F. H. O. M. K. M., 2012. Error Patterns in MLC NAND Flash Memory: Measurement, Characterization, and Analysis. LSI Corporation, 1110 American Parkway NE, Allentown, PA, 8(6), pp. 1-6.

[52] Li, J Quantitative data analysis techniques for data driven marketing. IACQUIRE, 2013.

[53] Saunders, M., Lewis, P., & Thornhill, A. 2009. Reaserch Methods for business students. Harlow: Pearson Education Limited.

[54] Golafshani understanding Reliability and Validity in qualitative research. The qualitative report volume 8, 2003.

[55] Mason, M., (2010). Sample size and saturation in PhD studies using Qualitative interviews, 63 paragraphs. Forum Qualitative Sozialforschung/Forum: Qualitative Social Research, 11(3), Art 8, http://nbn-resolving.de/urn:nbn:de:0114-fqs100387.

[56] Johannes D (2004), Joint Venture Contracting Relationships between Foreign and Local contractors in the construction and Engineering Industry of Hong Kong, published PhD of Philosophy Dissertation, RMIT University, Melbourn.

[57] Business dictionary, Research methodology definition, online, available on: www.BusinessDictionary.com , Accessed on 10/11/2017.

[58] Escalada M, Hoeng KL Guide line on how to conduct focus group discussion: Guide line manual for novice, 2009.

[59] Mndeme. I.S., Factors limiting effective implementation of training programs in parastatals organisations in Tanzania: A case study of Tanzania electric supply company limited, The open university of Tanzania, 2011.

[60] Burns, N., & Grove, S. K. Research Design and methodology, 1998. Retrieved from http://uir.unisa.ac.za/bitstream/handle/10500/1452/04chapter3.pdf.

[61] Parahoo, K. Nursing Research: Principles, process and Issues,. London: Macmillan Press Limited, 1997.

[62] Heiman, G. W. Basic Statistics for the Behavioral Sciences (6th ed.). Wadsworth Cengage Learning, 2011.

[63] Proctor, T. Essentials of Marketing Research. Essex, UK: Prentice-Hill, 2000.

[64] Wiegmann, D., Zhang, H., von Thaden, T., Sharma, G., & Gibbons, A. Culture: An Integrative Review. International Journal of Aviation, 14(2), 117-134, 2004.

[65] McNealy M.S. Strategies for Empirical Research in writing. New York Longman, 1999.

[66] Parahoo, K. Nursing Research: Principles, process and Issues,. London: Macmillan Press Limited, 1997.

[67] Annan, E. Challenges confronting the beneficiaries of the Vodafone/ UEW Educational Fund for future women leaders in science & technology in the University of Education. Winneba, Ghana, 2014.

[68] Judd, C. M., Smith, E. R., & Kiddler, L. H. Research Methods in Social Relations (16th ed.). New York: Harcourt Brace Jovanovich, 1991.

[69] Brown, J. D. Using Surveys in Language Programs. Cambridge: Cambridge University Press. Pune (Chakan plant ii). Scholarly research journal for interdisciplinary studies, Sep – Oct 2014. Vol – II/XIV.

[70] Choudhry, R. M., Fang, D., & Mohamed, S. The Nature of Culture: A Survey of the State of the Art. Safety Science, 45, 993-1012, 2007.

[71] Kothari, C. R. Reserch Methodology: Methods and Techniques (2nd ed.). New Delhi: New Age Internatioal Publisher, 2004.

[72] Carole, I. K., & Winterstein, A. G. Validity and reliability of measurement instruments used in research ReseaRch fundamentals. American Society of Health-System Pharmacists, 1, 2008.

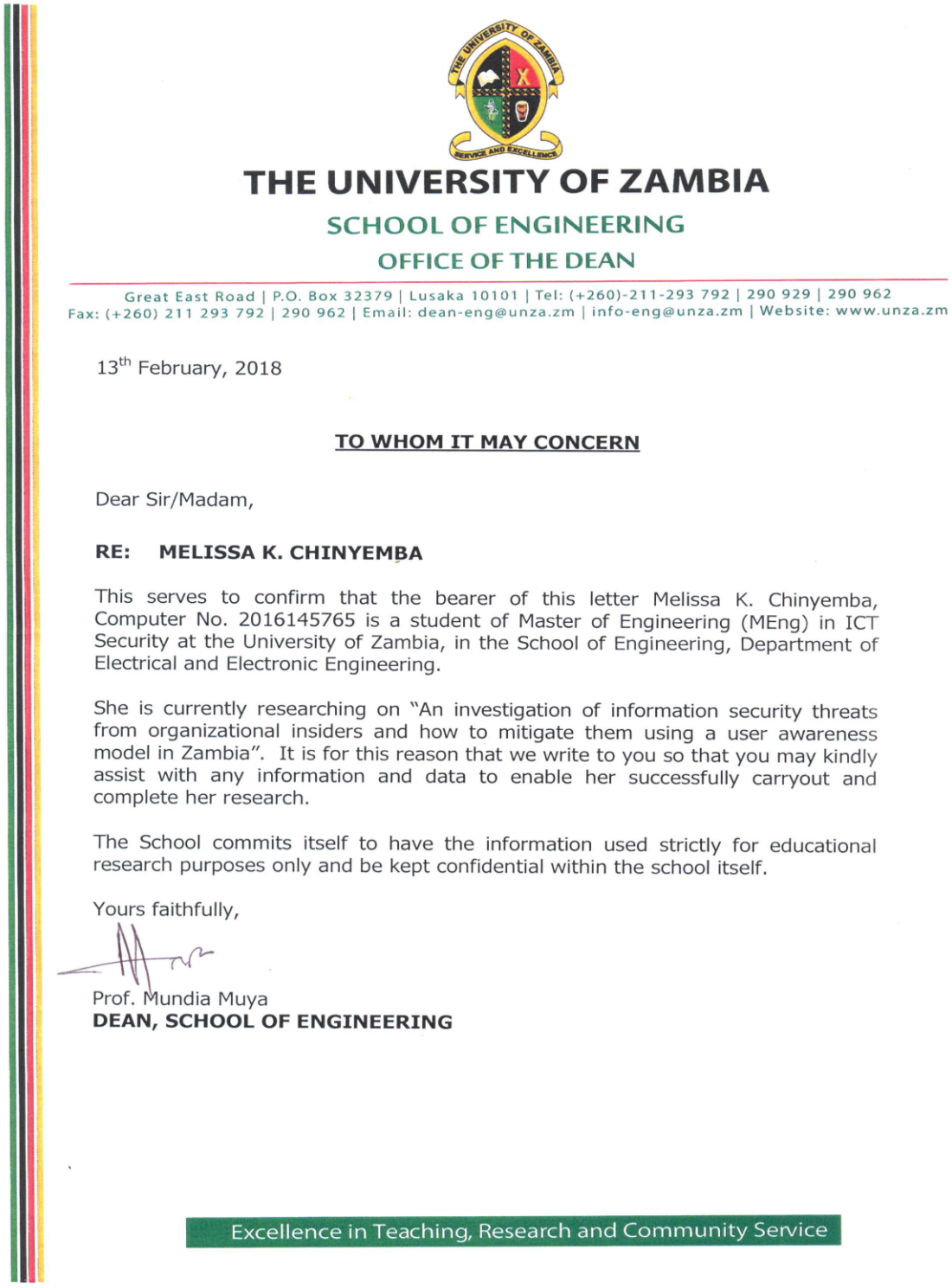
[73] Khorsan, R., & Crawford, C. External Validity and Model Validity: A Conceptual Approach for Systematic Review Methodology. Evidence-Based Complementary and Alternative Medicine, 11 pages, 2014.

[74] Kohlbacher, Florian. The Use of Qualitative Content Analysis in Case Study research, 89 paragraphs. Forum Qualitative Sozialforschung/Forum: Qualitative Social Research, 7(1), Art 21, 2005. http://nbn-resolving.de/urn:nbn:de:0114-fqs0601211.

[75] Yin, Robert K. Case study research, design and methods (3rd ed., vol5) Thousand Oaks: Sage 2003

APPENDICES

Appendix I: Introductory Letter from School



THE UNIVERSITY OF ZAMBIA

SCHOOL OF ENGINEERING

OFFICE OF THE DEAN

Great East Road | P.O. Box 32379 | Lusaka 10101 | Tel: (+260)-211-293 792 | 290 929 | 290 962
Fax: (+260) 211 293 792 | 290 962 | Email: dean-eng@unza.zm | info-eng@unza.zm | Website: www.unza.zm

13th February, 2018

TO WHOM IT MAY CONCERN

Dear Sir/Madam,

RE: MELISSA K. CHINYEMBA

This serves to confirm that the bearer of this letter Melissa K. Chinyemba, Computer No. 2016145765 is a student of Master of Engineering (MEng) in ICT Security at the University of Zambia, in the School of Engineering, Department of Electrical and Electronic Engineering.

She is currently researching on "An investigation of information security threats from organizational insiders and how to mitigate them using a user awareness model in Zambia". It is for this reason that we write to you so that you may kindly assist with any information and data to enable her successfully carryout and complete her research.

The School commits itself to have the information used strictly for educational research purposes only and be kept confidential within the school itself.

Yours faithfully,

Prof. Mundia Muya
DEAN, SCHOOL OF ENGINEERING

Excellence in Teaching, Research and Community Service

Appendix II: Letters of authority for data collection from some public organisations

ZESCO

Powering the Nation

Our Ref: A200/HRD/1169/2017

18 September 2017

Ms. Melisa K Chinyemba
C/O ZESCO Limited
ICT Security Department
LUSAKA

Dear Ms. Chinyemba,

RE: PERMISSION TO CONDUCT RESEARCH

Reference is made to the letter to us in which you requested ZESCO Management to grant you permission to carry out a research study on **"Mitigation of Cyber Threats from Malicious Internal Attackers: - A Case of ZESCO"**.

This serves to inform you that permission has been granted to you on the following terms and conditions:

1. That all information regarding the research should be handled with all the confidentiality it deserves and shall be used for academic purposes only.
2. The final report should be availed to the office of the undersigned before submission to your school for a go ahead in writing.
3. A copy of the final report shall be retained by ZESCO Limited for future reference.

Please fill in the attached form to indicate whether or not you are agreeable to these Terms and Conditions and return a copy to the office of the undersigned.

Yours Sincerely,
ZESCO LIMITED

CHILESHE M LUPUTA (MRS)
SENIOR MANAGER - HUMAN RESOURCE DEVELOPMENT

cc: Director – Human Resource
Human Resource Manager – S&CS
Training file

cml/cm

ZAMBIA INFORMATION
& COMMUNICATIONS
TECHNOLOGY
AUTHORITY

ZICTA/101/1/18

February 26, 2018

Melissa K. Chinyemba
The University of Zambia
P O Box 32379
Great East Road Campus
LUSAKA

Email: MChinyemba@zesco.co.zm

Dear Madam,

RE: PERMISSION FOR DATA COLLECTION ON MASTER'S RESEARCH "AN INVESTIGATION OF INFORMATION SECURITY THREATS FROM ORGANISATIONAL INSIDERS & HOW TO MITIGATE USING A USER AWARENESS MODEL IN ZAMBIA"

Reference is made to the above subject and your letter dated February 14, 2018.

With respect to your request, I hereby consent and authorize you to collect the required data for your research on the basis that the information is used strictly for educational research purposes and kept confidential.

For further information or clarification, please contact the Mr. Clyde Nkole - Acting Manager - Cyber Security on +260 211 244424 or email cnkole@zicta.zm.

Yours faithfully,
ZAMBIA INFORMATION AND COMMUNICATIONS TECHNOLOGY AUTHORITY

Mwenya Mutale (Mr.)
DIRECTOR TECHNOLOGY & ENGINEERING

cc : The Dean, School of Engineering - UNZA

cc : The Director General - ZICTA

HEAD OFFICE

Stand No. 4909 | Corner of United Nations Road & Independence Avenue
P.O. Box 36871, Lusaka
Telephone Lines: +260 21 1 244424 / 241236 / 244426 / 246702 / 244427
Fax Number: +260 21 1 246701

E-mail: info@zicta.zm
Complaints: complaints@zicta.zm
Website: www.zicta.zm
facebook.com/ZambiaICTAuthority

ROAD TRANSPORT AND SAFETY AGENCY

Head Office: P. O. Box 32167, Dedan Kimathi Road, Lusaka.
Tel: +260 211226 909 / 226 908 / 230 539 Fax: +260 211 231 601 Email: rtsa@zamnet.zm

RTSA 101/1/9

1st March, 2018.

The University of Zambia,
School of Engineering,
Department of Computer Science,
P.O Box 32379,
Lusaka.

Attention: Melissa K. Chinyemba
Cell No. : +260966955426

Dear Sir/Madam,

SUBJECT: PERMISSION FOR DATA COLLECTION ON MASTER'S RESEARCH "AN INVESTIGATION OF INFORMATION SECURITY THREATS FROM ORGANIZATIONAL INSIDERS AND HOW TO MITIGATE THEM USING A USER AWARENESS MODEL IN ZAMBIA.

We acknowledge receipt of your letter dated 14th February, 2018, requesting for authority to collect data from our Agency.

We have no objection in releasing information to you as long as the information provided is used for academic purposes only. We shall also be grateful if you could share your research findings with our Agency upon completion of your studies.

We would like to wish you good luck in your studies leading Masters of Engineering.

Yours faithfully,

Zindaba Soko
Director and Chief Executive Officer
Road Transport and Safety Agency

ZABS
Zambia Bureau Of Standards
"For Safety and Quality Assurance"

Lechwe House, Freedom Way - South End
P O Box 50259 ZA 15101, Ridgeway, Lusaka, Zambia
Tel: +260 211 231385 / 227075 / 221386
Telefax: +260 211 238483
E-mail: ceo@zabs.org.zm

ZabsDir/180/2018

6th March, 2018

Ms. Melissa K Chinyemba
School of Engineering
University of Zambia
LUSAKA

Dear Madam

Permission for Data Collection on Master's Research "An investigation of information Security threats from organizational insides and how to mitigate them using a user awareness model in Zambia"

Reference is made to your letter dated 14th February, 2018 on the above subject.

Kindly be informed that ZABS has no objection to your request of data collection in our organisation. For guidance on when to conduct your research, please get in touch with Mr. Davies Silungwe, Senior Administration Officer on 0977 510115.

Yours faithfully

MANUEL MUTALE
EXECUTIVE DIRECTOR

Approved
Kindly proceed to collect data.
02/05/2018

The Director
Centre for Information Communication Technology
University of Zambia
P.O. Box 32379
Lusaka

14th February, 2018

Dear Sir/Madam,

RE: Permission for Data collection on Master's Research "An Investigation into the Cyber Security Threats by Insiders: The Case of Public Organisations"

The above caption refers. According to the Master of Engineering Programs of the University of Zambia, it is a requirement for each student to submit his/her intended research work in their 2nd year of study. This is in partial fulfilment for the requirements of the degree of Master of Engineering in Information and Communications Technology (ICT) Security.

I therefore write to request permission for data collection in your organisation for my research as per the attached copy of the introduction letter from the University of Zambia.

Your consideration to this request will be highly appreciated.

Best Regards

Melissa K. Chinyemba
School of Engineering
University of Zambia
Lusaka, ZAMBIA

Contact number +260966955426
Email: MChinyemba@zesco.co.zm ***Cc:*** kaemelissa@gmail.com

UNIVERSITY OF ZAMBIA
DIRECTOR - C.I.C.T.
RECEIVED
25 APR 2018
P.O. BOX 32379, LUSAKA

Melissa K. Chinyemba

To: SIYUNYIK@zra.org.zm
Subject: RE: ISMS Gap Analysis & SoA Melz Version.xlsx

Received with thanks

Best Regards,

Eng. Melissa K. Chinyemba
ICT Security - Governance, Risk & Compliance (GRC)

Mobile: +260 966 955 426
Direct: +260 211 362 369
Email: Mchinyemba@zesco.co.zm
www.zesco.co.zm

From: SIYUNYIK@zra.org.zm [mailto:SIYUNYIK@zra.org.zm]
Sent: Friday, 11 May 2018 6:03 PM
To: Melissa K. Chinyemba
Subject: RE: ISMS Gap Analysis & SoA Melz Version.xlsx

As requested.

Kwibisa Siyunyi | Director – Internal Audit
Tel: +260 211 382200 | Telefax: +260 211 237 337 | Cell: +260 969 197 554
2nd Floor, Revenue House, Kabwe Roundabout, P.O. Box 35710,
Lusaka, Zambia | Email: SIyunyIK@zra.org.zm | Web: www.zra.org.zm

From: Melissa K. Chinyemba [mailto:MChinyemba@zesco.co.zm]
Sent: Friday, May 11, 2018 8:58 AM
To: A3 - KWIBISA SIYUNYI
Subject: ISMS Gap Analysis & SoA Melz Version.xlsx

Good morning Mr Kwibisa,

Sorry I fogot the statement of applicability requirements, so I have not been able to analyse the data and generate results.
Kindly fill in the first workbook named ISO 27K SOA – Req from the attached so that I can iupload the data to the tool.
Please baer with me, its pressure.

Best Regards,

1

Melissa K. Chinyemba

From: Sampa Chilanga <Sampa.Chilanga@zda.org.zm>
Sent: Wednesday, 4 April 2018 4:35 PM
To: Melissa K. Chinyemba
Cc: kaemelissa@gmail.com
Subject: DATA COLLECTION

Good Afternoon,
I have just received your letter for data collection. Please may you guide us on what specific information you would like from the ZDA so that we may assist you as soon as possible.

Sampa Jennifer Chilanga
Research and Policy Analyst |Zambia Development Agency| 0977-833666
Privatisation House, Nasser Road, P. O. Box 30819, Lusaka, Zambia|
Telephone: +260-211-220177|Fax: +260-211-225270|
Alt Email: sampa.chilanga@yahoo.com | https://www.linkedin.com/in/sampa-jennifer-chilanga-a3209a64
Website: http://www.zda.org.zm

1

Melissa K. Chinyemba

From: Andrew Kampolo <Andrew.Kampolo@zanaco.co.zm>
Sent: Monday, 14 May 2018 9:12 AM
To: Melissa K. Chinyemba
Subject: RESEARCH QUESTIONNAIRE
Attachments: Andrew.Kampolo_180514-081927-ea2.pdf

Dear Melissa,

Kindly find attached the as agreed.

Best regards

Andrew M. Kampolo – CISA
IT Risk Management Head

zanaco

Risk Division | Head Office | Zanaco | P.o.Box 33611 | Cairo Road | Lusaka, Zambia
General Line: +260 211 228979 Ext: 1336 | Mobile: +260 975 860675|
Email : andrew.kampolo@zanaco.co.zm |
Web: www.zanaco.co.zm

Download NOW

Andrew Kampolo
Head - IT Risk Management

zanaco

Head Office | Zanaco | Chainda Place | P.O. Box 33611 | Lusaka, Zambia
Tel: +260 211 425 650 | Ext: 5492 | Mobile: +260 975 860 675
Email: Andrew.Kampolo@zanaco.co.zm | Web: www.zanaco.co.zm

Download NOW

Appendix III: Questionnaire No 1 – Survey

The University of Zambia

School of Engineering

An investigation into Cyber Security threats posed by insiders: A case of Public Organisations

---

By Melissa K. Chinyemba (2016145765)

Master of Engineering – ICT Security

For further details or any queries, kindly get in touch on 0966 955426

Dear Respondent,

I am a student at the University of Zambia in my final stage pursuing a Master of Engineering – ICT Security. As partial fulfillment for the award of a Master's degree, I am conducting a baseline study on: "**An investigation into Cyber Security threats posed by insiders: A case of Public Organisations"**

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. Jackson Phiri (0966 693 731)

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

1) **Sex:** **(1**) Male ☐ (2) Female ☐

2) **Age in years.**

(1) 18 – 22 ☐ (4) 30 – 34 ☐

(2) 22 – 26 ☐ (5) 34 – 40 ☐

(3) 26 – 30 ☐ (6) 40 and above ☐

3) **Marital status**

(1) Single ☐ (4) Separated ☐

(2) Married ☐ (5) Divorced ☐

(3) Widowed ☐

4) **Level of education**

(1) Secondary ☐ (3) University ☐

(2) College ☐ (4) others ☐

5) **Line of specialty,** please specify…….....

6) **Professional certifications,** please list them: …….....

……..

7) **What is your organization's Primary industry?**

(1) Government Agency/Authority ☐ (4) Health Care ☐

(2) Telecommucations/ICT ☐ (5) Banking ☐

(3) Energy/Utility ☐ (6) Higher Institution of learning ☐

8) What is your organization's size in terms of its overall workforce, including employees and outside individuals such as contractors, consultants and interns?

(1) Fewer than 500 ☐ (3) 1000 – 4999 ☐

(2) 500 - 999 ☐ (4) 5000 & above ☐

9) **What is your primary role in the organization?**

1) Security manager/ Director/CSO/CISO ☐
2) ICT manager/ Director/CIO ☐
3) Risk Manager/ Director ☐
4) Compliance officer/ Auditor ☐
5) ICT Specialist ☐
6) Human Resources Manager/Officer ☐
7) Legal professional ☐
8) ICT Security Analyst /Officer ☐
9) Help desk agent / technician ☐
10) System/Database administrator ☐
11) Finance Manager /Officer ☐

12) If others, please specify……..

2. Part B: Please tick in the box as appropriate

1) The Cyber/ICT Security department is functioning under the control of:

- ☐ 1) A Chief security Officer with professional and academic ICT Security qualification
- ☐ 2) A Chief ICT Security Officer certified in CCISO or CISSP
- ☐ 3) A college graduate with several years of experience
- ☐ 4) A university graduate without Cyber/ICT Security background

2) The Head of Cyber/ICT Security department at your organisation reports to:

- ☐ 1) Chief Executive Officer
- ☐ 2) Cyber/ICT Security committee
- ☐ 3) Director IT/IS/ICT
- ☐ 4) IT/IS/ICT Senior Manager

3) The number of staff in the Cyber/ICT Security department/Section at your organisation is:

- ☐ 1) Between 1 to 5
- ☐ 2) Between 6 to 10
- ☐ 3) Between 10 to 15
- ☐ 4) More than 15

5) Does your Cyber/ICT Security department have a buy-in from the executive/senior management?

- ☐ 1) Yes it does
- ☐ 2) No it doesn't
- ☐ 3) Am not sure
- ☐ 4) None of the above

6) How is your Cyber/ICT Security department supported by the executive/senior management?

- ☐ 1) Very well Supported
- ☐ 2) Adequately Supported
- ☐ 3) Moderately Supported
- ☐ 4) Poorly Supported

7) How is Cyber/ICT Security department funded at your Organisation?

- ☐ 1) Very well-funded
- ☐ 2) Adequately funded
- ☐ 3) Moderately funded
- ☐ 4) Poorly funded

8) Staff Establishment

Position	Approved Establishment	Actual	Variance
CISO/Director ICT Security			
Cyber/ICT Security Senior Manager(s)			
Cyber/ICT Security Manager(s)			
Senior Cyber/ICT Security Officers			
Cyber/ICT Security Officers			

Part C: Questionnaire for assessing the extent to which internal Cyber/ICT Security controls assurance enhances corporate governance.

In this part of the questionnaire you are expected to answer by choosing one of the options:

Code:	**1**	**2**	**3**	**4**	**5**
For:	**Strongly Disagree**	**Disagree**	**Not Sure**	**Agree**	**Strongly Agree**

SN.		**1**	**2**	**3**	**4**	**5**
01	Your organisation has adopted, implemented and enforced the international ISMS standards and framework such as ISO 27001 and COBIT for security.					
02	Cyber/ICT Security has a risk-based plan that determines the priorities of the Cyber/ICT Security activity, consistent with the organization's goals.					
03	The Chief Cyber/ICT Security Officer (CISO) ensures that Cyber/ICT Security resources are appropriate, sufficient, and effectively deployed to achieve the approved plan.					
04	The Cyber/ICT Security activity assist the company in maintaining effective controls by evaluating their effectiveness and efficiency and by promoting continuous improvement					
05	Cyber/ICT Security Officers check that internal controls exist and are working effectively					
06	Cyber/ICT Security Officers are alert to the significant risks that might affect objectives, operations, or resources.					

07	Cyber/ICT Security helps in the achievement of the company's strategic objectives.					
08	Cyber/ICT Security ensures that there is compliance with laws, regulations, policies, procedures, and contracts by the company					
09	Confidentiality and integrity of financial, strategic, and operational information is assured by CISO					
10	Cyber/ICT Security has greatly helped to safeguard assets and minimize loss at our organisation					
11	Cyber/ICT Security carry out ICT risk assessments that has helped Management at our Organisation					
12	Cyber/ICT Security at our organisation issue reports in a useful timely?					
13	Cyber/ICT Security staff are given regular in-house awareness and training in security practice standards					
14	Not all Cyber/ICT Security staff at our Organisation have experience and are certified in Cyber/ICT Security profession					
15	What is the most positive or negative attribute that Cyber/ICT Security Officers have exhibited?------ ---------- ----------					

Part D: Questionnaires for assessing the influence of Cyber/ICT Security recommendations on corporate governance

This part of the questionnaire you are expected to use the same Likert scale as in part B as follows:

Code:	**1**	**2**	**3**	**4**	**5**
For:	**Strongly Disagree**	**Disagree**	**Not Sure**	**Agree**	**Strongly Agree**

SN.		**1**	**2**	**3**	**4**	**5**
01	The Cyber/ICT Security activity assess and make appropriate and value adding recommendations which are implemented by management on a timely basis to improve the organization's governance processes					

02	The Chief Cyber/ICT Security Officer (CISO) communicates results to the appropriate parties timely for consideration.					
03	Management accepts responsibility for monitoring corrective action on vulnerabilities reported by Cyber/ICT Security.					
04	The Cyber/ICT Security executive establishes and maintains a system to monitor the disposition of results communicated to management.					
05	Cyber/ICT Security have clear and positive relationship with management that allows it to communicate openly and confidently without fear of repercussions					
06	Management views Cyber/ICT Security function as an impediment to fulfilling its objective on time					
07	The Cyber/ICT Security budget includes adequate funds for professional development and the planned use of external experts.					
08	The degree of response to Cyber/ICT Security report by senior management is satisfactory					
09	What is it that Cyber/ICT Security officials should do or should not do to improve its relevancy at your Organisation?---------- ----------					

Part E: Questionnaire on the independence and objectivity of Cyber/ICT Security activity in the organisation as a mechanism of governance.

The key to filling this section is given below. Please tick the most appropriate option for you. This part of the questionnaire you are expected to use the same Likert scale as in part B as follows:

Code:	**1**	**2**	**3**	**4**	**5**
For:	**Strongly Disagree**	**Disagree**	**Not Sure**	**Agree**	**Strongly Agree**

SN.		**1**	**2**	**3**	**4**	**5**
01	The department has a charter approved by the board that gives it its mandate and independence with a formally defined purpose, authority,					

	and responsibility of the Cyber/ICT Security activity in line with the Mission of Cyber/ICT Security					
02	Cyber/ICT Security Officers are professionals and competent to act independently and objectively in the performance of their work.					
03	The relationship between Cyber/ICT Security and employees is viable and professional?					
04	The Cyber/ICT Security activity is free from interference in determining the scope of Cyber/ICT Security, performing work, and communicating results.					
05	Cyber/ICT Security Officers have an impartial, unbiased attitude and avoid any conflict of interest.					
06	If independence or objectivity is impaired in fact or appearance, the details of the impairment are disclosed to appropriate parties.					
07	Cyber/ICT Security Officers provide consulting services relating to operations for which they had previous responsibilities.					
08	If Cyber/ICT Security Officers have potential impairments to independence or objectivity relating to proposed consulting services, disclosure is made to the engagement client prior to accepting the engagement					
09	Cyber/ICT Security function sometimes faces interference from management in determining its scope and communicating results.					
10	Cyber/ICT Security at our organisation have access to all records and books without interference from line managers					
11	Cyber/ICT Security staff are required to review all departments in the organisation					
12	Cyber/ICT Security Function report at a very senior level in the Organisation					
13	Cyber/ICT Security have no personal or professional involvement with or allegiance to the asset being protected and maintains an un-biased and impartial mindset in regard to all engagements at our organisation					

14	Is Cyber/ICT Security function seen and act independently at your company?, YES or NO ----------

Part F: Questionnaire on insider threats and security activity in the organisation

Please tick in the boxes as appropriate

1) Which category of insider are you the most concerned with as being the most detrimental to your organization? Select the best answers.

- ☐ Negligent contractor
- ☐ Negligent employee
- ☐ Unscreened / new employee
- ☐ Malicious contractor
- ☐ Malicious employee
- ☐ A former Employee
- ☐ Disgruntled employee
- ☐ Security-unaware/ employee / Contractor
- ☐ Security-uninformed contractor

2) What are you most concerned about as relates to an insider threat? Select all that apply.

- ☐ Fraud or abuse
- ☐ Exposure of confidentiality
- ☐ Business information
- ☐ Compromise of Personally PII
- ☐ Loss of competitive advantage
- ☐ Lack of continuity Plans
- ☐ Reputation damage
- ☐ Other: Specify……
- ☐ Lack of clear communication channels
- ☐ Lack comprehensive access control
- ☐ Lack of information Classification Policy
- ☐ Sabotage
- ☐ Theft of IP
- ☐ Compromise of HR information
- ☐ Unclearly defined organisation rules

3) Can you place a financial value in U.S. dollars on your organization's potential loss from an insider threat?

- ☐ 1) Under $99,999
- ☐ 2) $100,000 to $249,000
- ☐ 3) $250,000 to $499,000
- ☐ 4) $500,000 to $999,999
- ☐ 5) $1 to $2.4M
- ☐ 6) $2.5 to $5M
- ☐ 7) $5M and above
- ☐ 8) Unknown/Unsure

4) What percentage of your ICT budget are you currently spending for prevention and detection of insider incidents/attacks?

☐ 1) Less than 5%
☐ 2) 5–7%
☐ 3) 7–10%
☐ 4) More than 10%
☐ 5) Unknown

5) What do you estimate this percentage might be in the next twelve months?

☐ 1) Less than 5%
☐ 2) 5–7%
☐ 3) 7–10%
☐ 4) More than 10%
☐ 5) Unknown

6) Does your organisation have the ability to prevent/deter an insider incident/attack?

☐ 1) Yes ☐ 2) Not Sure ☐ 3) No

7) What tools or techniques are you using to prevent/deter insider threats before they become an actual incident or attack?

☐ Administrative policies & procedures
☐ Workforce monitoring
☐ Internal controls
☐ DLP
☐ Internal audits
☐ Whistleblower
☐ Other

8) What Administrative policies & procedures are you using to prevent, detect and mitigate actual insider threats incident or attack? Select all that apply.

☐ ICT Security Policy & Procedures
☐ Comprehensive NDA Policy
☐ Employee screening Policy
☐ Exit Policy /Procedure
☐ Clear Desk Policy
☐ None of the above
☐ Other. Specify: …..……...
☐ Awareness Policy & Procedures
☐ Information classification Policy
☐ Role-base access control policy
☐ Acceptable use policy
☐ Access Control Policy

9) Does your ICT /Cyber Security/HR department mandate a screening and underground check for prospective employees before they are employed?

- ☐ 1) Yes
- ☐ 2) No
- ☐ 3) Partially
- ☐ 4) Not Sure

10) How often do you review the policies and procedure? Select all that apply

- ☐ 1) Quarterly
- ☐ 2) Bi-annually
- ☐ 3) Annually
- ☐ 4) Whenever there is change
- ☐ 5) Never
- ☐ 6) There is no need to review

11) How often do you conduct user awareness? Select all that apply

- ☐ 1) Weekly
- ☐ 2) Monthly
- ☐ 3) Quarterly
- ☐ 4) Bi-annually
- ☐ 7) Whenever there is change
- ☐ 8) Not sure
- ☐ 5) Annually
- ☐ 6) Never

12) Who is covered under awareness/training scope?

- ☐ 1) Unionized employees only
- ☐ 2) Management employees only
- ☐ 3) Computer users only
- ☐ 4) System administrators
- ☐ 5) IT/ICT Security staff only
- ☐ 6) IT/ICT staff only
- ☐ 7) Everyone
- ☐ 8) No one

13) Do you keep record of the signed acknowledgements from users who have undergone awareness and read the security policies as proof of enforcement and delivery?

- ☐ 1) YES
- ☐ 2) Not Sure
- ☐ 3) No

14) What factors do you feel are limiting your ability to prevent/deter an insider incident/attack? Select all that apply.

- ☐ Lack of training
- ☐ Other
- ☐ Lack of technology solutions
- ☐ Lack of budget
- ☐ Lack of appropriate policies & procedures
- ☐ Lack of internal specialized staff
- ☐ Not a priority for my organization

15) To help determine the biggest gaps in your organization, draw up a report card. In the following areas, give yourself an "A" if you are addressing that area, an "F" if you are ignoring it:

- ☐ Policies
- ☐ Procedures
- ☐ Comprehensive Awareness
- ☐ Comprehensive Training
- ☐ Technology
- ☐ Administrative
- ☐ Executive support
- ☐ Employee screening

16) How effective do you feel your prevention measures are?

- ☐ 1) Very effective (i.e., we have proven tools/techniques against attack)
- ☐ 2) Effective (i.e., we are confident we have selected the best tools/techniques but have not used them operationally)
- ☐ 3) Not effective (i.e., we are in the process of re-evaluating our processes)
- ☐ 4) Not applicable (i.e., we are not concerned about insider threats)

17) What tools or techniques do you use to detect insider incidents/attacks? Select all that apply.

- ☐ Internal audits
- ☐ Internal network monitoring
- ☐ Centralized log management
- ☐ SIEM tools
- ☐ External network Monitoring
- ☐ Other. Specify: ……
- ☐ Data loss prevention/protection
- ☐ Monitoring of third parties
- ☐ Whistleblower
- ☐ Monitoring of employees

18) Does your incident response plan have special provisions for incidents involving insiders?

- [ ] 1) Yes, we have a formal incident response plan with special provisions for insiders
- [ ] 2) No, our formal incident response plan does not have special provisions for insiders
- [ ] 3) No, we have no formal incident response plan
- [ ] 4) Unknown

19) Have you ever experienced an actual insider incident/attack in your organisation?

- [ ] 1) Yes
- [ ] 2) Not Sure
- [ ] 3) No

20) If Yes to 19 above, how would you class the type of the insider attack?

- [ ] 1) Fraud
- [ ] 2) Sabotage
- [ ] 3) IP Theft
- [ ] 4) Other

21) From the actual or estimated start of the incident/attack, how long did it take you to detect/mitigate?

- [ ] 1) Less than an hour
- [ ] 2) 1 – 8 hours
- [ ] 3) <1 – 7 days <7-12 months
- [ ] 4) <1 – 4 weeks
- [ ] 5) <1 – 6 months
- [ ] 6) More than a year
- [ ] 7) Unknown/Unsure

22) What do you estimate was the extent of your (worst) loss in U.S. dollars?

- [ ] 1) Under $500, 000
- [ ] 2) $500,001 to $ 1M
- [ ] 3) <$ 1M to $5M
- [ ] 4) Over $5M
- [ ] 5) Unknown / Unsure
- [ ] 6) None of the above

23) Does your organisation have an ICT/ Cyber Security policy and procedure which are aligned to the corporate strategy?

- [ ] 1) Yes
- [ ] 2) Not Sure
- [ ] 3) No

24) Does your organisation have a mandatory Non-Disclosure Agreement (NDA) Policy?

- [ ] 1) Yes
- [ ] 2) Not Sure
- [ ] 3) No

25) Does your organisation mandate exit interviews before paying of the benefits of any leaving employees/contractors?

☐ 1) Yes ☐ 2) Not Sure ☐ 3) No

26) Does the NDA policy have a clause to deter the exiting employees/contractors from leaking the organisational information?

☐ 1) Yes ☐ 2) Not Sure ☐ 3) No

27) Does the NDA policy have a clause to deter the exiting employees from sabotaging the organisation?

☐ 1) Yes ☐ 2) Not Sure ☐ 3) No

28) What's the Policy for user access rights deactivation after termination of contract?

☐ 1) Immediately
☐ 2) After a couple hours
☐ 3) After a day
☐ 4) After a week or Month
☐ 5) After paying off their dues
☐ 6) Never

Part G: Assessing Your Vulnerability to Insider Threats

1) Why do you think an insider would attack their own employers?

……

……

2) What do you think would lead to insider attack in your organisation?

……

……

3) Which of the indicators has your organisation adequately addressed in mitigating insider attacks?

……..

……

4) What information would an adversary target in your organisation?

……

……..

5) What systems contain the information that attackers would target?

……

……

6) Who has access to the critical information and systems?

……

……

7) How would an adversary target that individual?

……

……

8) What would be the easiest way to compromise an insider in your organisation?

……

……

9) How would someone extract the information?

……

……

10) What measures or solutions should your ICT use/put in place to prevent these attacks?

……

……

11) What measures or solutions can ICT use to detect these attacks? .....
……

12) What gaps exist in how you are dealing with insider threats in your organisation?
……

13) What are the highest-priority items/assets to focus on?
……

14) Does our current budget appropriately address insider threats?
……

15) Should your organisation adjust current resources and budget to address insider threats?
……

16) What would a security roadmap that includes insider threats look like?
……

Thank you so much for contributing positively to this research paper.

May God richly bless you!

Appendix IV: Questionnaire No 2 - Gap Analysis

Statement of Applicability of ISO/IEC 27001:2013 Annex A controls				
Annex A reference	**Control title**	**Control description**	**Additional Questions**	**Function**
A.5	**Information Security Policies**			
A5.1	**Management direction for information security**	**To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.**		
A.5.1.1	Policies for information security	An information security policy document shall be approved by management, and published and communicated to all employees and relevant external parties.	Does your institution have an information security policy that has been approved by management?	Top Management
A.5.1.2	Review of the policies for information security	The information security policy shall be reviewed at planned intervals or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.	Does your institution review the policy at defined intervals to encompass significant change and monitor for compliance?	Top Management

A.6	**Organization of information security**			
A.6.1	**Internal Organization**	**To manage information security within the organization.**		
A.6.1.1	Information security roles and responsibilities	Management shall actively support security within the organization through clear direction, demonstrated commitment, explicit assignment, and acknowledgement of information security responsibilities.		Top Management
A.6.1.2	Segregation of duties	Information security activities shall be co-ordinated by representatives from different parts of the organization with relevant roles and job function.	Does your information security function have the authority it needs to manage and ensure compliance with the information security program?	CISO
A.6.1.3	Contact with authorities	All information security responsibilities are clearly defined.	Does your institution have an individual with enterprise-wide (campus) information security responsibility and authority written in their job description, or equivalent? Note: This may be the CIO, CISO, CSO, or other.	HR

A.6.1.4	Contact with special interest groups	A management authorization process for new information processing facilities shall be defined and implemented.	Is responsibility clearly assigned for all areas of the information security architecture, compliance, processes, and audits?	CISO
A.6.1.5	Information security in project management	Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified and regularly reviewed.	Is there a formal process for having the individual with information security responsibility assess and sign off on appropriate hardware, software, and services, ensuring they follow security policies and requirements?	CISO
A.6.2	Contact with authorities	Appropriate contacts with relevant authorities shall be maintained.	Does your institution maintain relationships with local authorities?	Administration
A.6.1.7	Contact with special interest groups	Appropriate contacts with special interest groups or other specialist security forums and professional associations shall be maintained.	Does your institution participate with local or national security groups (e.g., REN-ISAC, EDUCAUSE, InfraGard, Information Systems Security Association, etc.)?	IT
A.6.1.8	Independent review of information security	The organization's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes, and procedures for information security)	Does your institution have independent security reviews completed at planned intervals or when	CISO

		shall be reviewed independently at planned intervals, or when significant changes to the security implementation occur.	significant changes to the environment occur?	
A6.2	**External parties**	**To maintain the security of organization's information and information processing facilities that are accessed, processed, communicated to, or managed by external parties.**		
A.6.2.1	Identification of risks related to external parties	The risks to the organization's information and information processing facilities from business processes involving external parties shall be identified and appropriate controls implemented before granting access.	Does your institution have an ICT risk management program?	CISO
A.6.2.2	Addressing security when dealing with customers	All identified security requirements shall be addressed before giving customers access to the organization's information or assets.	Does your institution have a process for identifying and assessing reasonably foreseeable internal and external ICT risks to the security, confidentiality, and/or integrity of any electronic, paper, or other records containing sensitive information?	IT

A.6.2.3	Addressing security in third party contracts	Agreements with third parties involving accessing, processing, communicating or managing the organization's information or information processing facilities, or adding products or services to information processing facilities shall cover all relevant security requirements.	Does your organization conduct routine risk assessments to identify the key objectives that need to be supported by your information security program?	Finance
A.7	**Human resources security**			
A.7.1	**Prior to employment**	**To ensure that employees, contractors and third party users understand their responsibilities, and are suitable for the roles they are considered for, and to reduce the risk of theft, fraud or misuse of facilities.**		
A.7.1.1	Roles and responsibilities	Security roles and responsibilities of employees, contractors and third party users shall be defined and documented in accordance with the organization's information security policy.	Do all individuals interacting with university systems receive information security awareness training?	HR
A.7.1.2	Screening	Background verification checks on all candidates for employment, contractors, and third party users shall be carried out in accordance with relevant laws, regulations and ethics, and proportional to the business requirements, the classification of the information to be accessed, and the perceived risks.	Does your institution conduct specialized role-based training?	HR

A.7.1.3	Terms and conditions of employment	As part of their contractual obligation, employees, contractors and third party users shall agree and sign the terms and conditions of their employment contract, which shall state their and the organization's responsibilities for information security.	Do the information security programs clearly state responsibilities, liabilities, and consequences?	HR
A.7.2	**During employment**	**To ensure that all employees, contractors and third party users are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support organizational security policy in the course of their normal work, and to reduce the risk of human error.**		
A.7.2.1	Management responsibilities	Management shall require employees, contractors and third party users to apply security in accordance with established policies and procedures of the organization.		HR
A.7.2.2	Information security awareness, education and training	All employees of the organization and, where relevant, contractors and third-party users, shall receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant for their job function.		Training
A.7.2.3	Disciplinary process	There shall be a formal disciplinary process for employees who have committed a security breach.		HR

A.7.3	**Termination or change of employment**	**To ensure that employees, contractors and third party users exit an organization or change employment in an orderly manner.**		
A.7.3.1	Termination responsibilities	Responsibilities for performing employment termination or change of employment shall be clearly defined and assigned.		HR
A.7.3.2	Return of assets	All employees, contractors and third party users shall return all of the organization's assets in their possession upon termination of their employment, contract or agreement.		HR
A.7.3.3	Removal of access rights	The access rights of all employees, contractors and third party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.		HR
A.8	**Asset Management**			
A.8.1	**Responsibility for assets**	**To achieve and maintain appropriate protection of organizational assets.**		
A.8.1.1	Inventory of assets	All assets shall be clearly identified and an inventory of all important assets drawn up and maintained.	Has your organization identified critical information assets and the functions that rely on them?	CISO

A.8.1.2	Ownership of assets	All information and assets associated with information processing facilities shall be owned by a designated part of the organization.	Does your institution classify information to indicate the appropriate levels of information security?	CISO
A.8.1.3	Acceptable use of assets	Rules for the acceptable use of information and assets associated with information processing facilities shall be identified, documented, and implemented.		CISO
A.8.2	**Information classification**	**To ensure that information receives an appropriate level of protection.**		
A.8.2.1	Classification guidelines	Information shall be classified in terms of its value, legal requirements, sensitivity and criticality to the organization.		CISO
A.8.2.2	Information labelling and handling	An appropriate set of procedures for information labelling and handling shall be developed and implemented in accordance with the classification scheme adopted by the organization.		CISO
A9	**Access Control**			
A9.1	**Business requirement for access control**	**To control access to information.**		
A9.1.1	Access control policy	An access control policy shall be established, documented, and reviewed		IT

		based on business and security requirements for access.		
A9.2	**User access management**	**To ensure authorized user access and to prevent unauthorized access to information systems.**		
A9.2.1	User registration	There shall be a formal user registration and de-registration procedure in place for granting and revoking access to all information systems and services.	Does your institution have an access control policy for authorizing and revoking access rights to information systems?	IT
A9.2.2	Privilege management	The allocation and use of privileges shall be restricted and controlled.	Does your institution have a process in place for granting and revoking appropriate user access?	IT
A9.2.3	User password management	The allocation of passwords shall be controlled through a formal management process.	Does your institution have a password management program that follows current security standards?	IT
A9.2.4	Review of user access rights	Management shall review users' access rights at regular intervals using a formal process.	Does your institution have procedures to regularly review users' access to ensure only needed privileges are applied?	IT
A9.3	**User responsibilities**	**To prevent unauthorized user access, and compromise or theft of information and information processing facilities.**		

A9.3.1	Password use	Users shall be required to follow good security practices in the selection and use of passwords.	Does your institution employ specific measures to secure remote access services?	IT
A9.3.2	Unattended user equipment	Users shall ensure that unattended equipment has appropriate protection.	Does your institution employ technologies to block or restrict unencrypted sensitive information from traveling to untrusted networks?	IT
A9.3.3	Clear desk and clear screen policy	A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted.	Does your institution have mechanisms in place to manage digital identities (accounts, keys, tokens) throughout their life cycle, from registration through termination?	IT
A9.4	**Network access control**	**To prevent unauthorized access to networked services.**		
A9.4.1	Policy on use of network services	Users shall only be provided with access to the services that they have been specifically authorized to use.	Is there a policy in place to restrict the sharing of passwords?	IT
A9.4.2	User authentication for external connections	Appropriate authentication methods shall be used to control access by remote users.	Does your institution prohibit use of generic accounts with privileged access to systems?	IT

A9.4.3	Equipment identification in networks	Automatic equipment identification shall be considered as a means to authenticate connections from specific locations and equipment.	Does your institution have an authentication system in place that applies higher levels of authentication to protect resources with higher levels of sensitivity?	IT
A9.4.4	Remote diagnostic and configuration port protection	Physical and logical access to diagnostic and configuration ports shall be controlled.	Does your institution have an authorization system that enforces time limits lockout on login failure and defaults to minimum privileges?	IT
A9.4.5	Segregation in networks	Groups of information services, users and information systems shall be segregated on networks.	Does your institution have standards for isolating sensitive data and procedures and technologies in place to protect it from unauthorized access and tampering?	IT
A9.4.6	Network connection control	For shared networks, especially those extending across the organization's boundaries, the capability of users to connect to the network shall be restricted, in line with the access control policy and requirements of the business applications (see 11.1).	Does your institution have usage guidance established for mobile computing devices (regardless of ownership) that store, process, or transmit institutional data?	IT

A9.4.7	Network routing control	Routing controls shall be implemented for networks to ensure that computer connections and information flows do not breach the access control policy of the business applications.	Does your institution require encryption on mobile (i.e., laptops, tablets, etc.) computing devices?	IT
A9.5	**Operating system access control**	**To prevent unauthorized access to operating systems.**		
A9.5.1	Secure log-on procedures	Access to operating systems shall be controlled by a secure log-on procedure.		IT
A9.5.2	User identification and authentication	All users shall have a unique identifier (user ID) for their personal use only, and a suitable authentication technique shall be chosen to substantiate the claimed identity of a user.		IT
A9.5.3	Password management system	Systems for managing passwords shall be interactive and shall ensure quality passwords.		IT
A9.5.4	Use of system utilities	The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.		IT
A9.5.5	Session time-out	Inactive sessions shall be shut down after a defined period of inactivity.		IT
A9.5.6	Limitation of connection time	Restrictions on connection times shall be used to provide additional security for high-risk applications.		IT
A9.6	**Application and**	**To prevent unauthorized access to information held in application systems.**		

	information access control			
A9.6.1	Information access restriction	Access to information and application system functions by users and support personnel shall be restricted in accordance with the defined access control policy.		IT
A9.6.2	Sensitive system isolation	Sensitive systems shall have a dedicated (isolated) computing environment.		IT
A9.7	**Mobile computing and Teleworking**	**To ensure information security when using mobile computing and teleworking facilities.**		
A9.7.1	Mobile computing and communications	A formal policy shall be in place, and security measures shall be adopted to protect against the risks of using mobile computing and communication facilities.		CISO
A9.7.2	Teleworking	A policy, operational plans and procedures shall be developed and implemented for teleworking activities.	Does your institution have a telework policy that addresses multifactor access and security requirements for the end point used?	CISO
A10	**Cryptography**			
A10.1	Cryptographic controls	Does your institution use appropriate/vetted encryption methods to protect sensitive data in transit?	Does your institution use appropriate/vetted encryption methods to protect sensitive data in transit?	CISO

A10.1.1	Policy on the use of cryptographic controls	A policy on the use of cryptographic controls for protection of information shall be developed and implemented.	Do your policies indicate when encryption should be used (e.g., at rest, in transit, with sensitive or confidential data, etc.)?	CISO
A10.1.2	Key management	A policy on the use, protection and lifetime of cryptographic keys shall be developed and implemented through their whole lifecycle.	Are standards for key management documented and employed?	CISO
A.11	**Physical and environmental security**			
A11.1	**Secure areas**	**To prevent unauthorized physical access, damage and interference to the organization's premises and information.**		
A11.1.1	Physical security perimeter	Security perimeters (barriers such as walls, card controlled entry gates or manned reception desks) shall be used to protect areas that contain information and information processing facilities.	Do your institution's data centers include controls to ensure that only authorized parties are allowed physical access?	Administration
A11.1.2	Physical entry controls	Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.	Does your institution have preventative measures in place to protect critical hardware and wiring from natural and man-made threats?	Administration
A11.1.3	Securing offices, rooms and facilities	Physical security for offices, rooms, and facilities shall be designed and applied	Does your institution have a process for issuing keys, codes, and/or cards	Administration

			that require appropriate authorization and background checks for access to these sensitive facilities?	
A11.1.4	Protecting against external and environmental threats	Physical protection against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster shall be designed and applied.	Does your institution follow vendor-recommended guidance for maintaining equipment?	Administration
A11.1.5	Working in secure areas	Physical protection and guidelines for working in secure areas shall be designed and applied.	Does your institution have a media-sanitization process that is applied to equipment prior to disposal, reuse, or release?	Administration
A11.1.6	Public access, delivery and loading areas	Access points such as delivery and loading areas and other points where unauthorized persons may enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.	Are there processes in place to detect the unauthorized removal of equipment, information, or software?	Administration
A11.2	**Equipment security**	**To prevent loss, damage, theft or compromise of assets and interruption to organization's activities.**		
A11.2.1	Equipment siting and protection	Equipment shall be sited and protected to reduce the risks from environmental	Do your institution's data centers include controls to ensure that only	Administration

		threats and hazards, and opportunities for unauthorized access.	authorized parties are allowed physical access?	
A11.2.2	Supporting utilities	Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.	Does your institution have preventative measures in place to protect critical hardware and wiring from natural and man-made threats?	Administration
A11.2.3	Cabling security	Power and telecommunications cabling carrying data or supporting information services shall be protected from interception or damage.	Does your institution have a process for issuing keys, codes, and/or cards that require appropriate authorization and background checks for access to these sensitive facilities?	Administration
A11.2.4	Equipment maintenance	Equipment shall be correctly maintained to enable its continued availability and integrity.	Does your institution follow vendor-recommended guidance for maintaining equipment?	IT
A11.2.5	Security of equipment off-premises	Security shall be applied to off-site equipment taking into account the different risks of working outside the organization's premises.		IT
A11.2.6	Secure disposal or re-use of equipment	All items of equipment containing storage media shall be checked to ensure that any sensitive data and licensed	Does your institution have a media-sanitization process that is applied to equipment prior to	IT

		software has been removed or securely overwritten prior to disposal.	disposal, reuse, or release?	
A11.2.7	Removal of property	Equipment, information or software shall not be taken off-site without prior authorization.	Are there processes in place to detect the unauthorized removal of equipment, information, or software?	Administration
A12	**Operations Security**			
A12.1	**Operational procedures and responsibilities**	**To ensure the correct and secure operation of information processing facilities.**		
A12.1.1	Documented operating procedures	Operating procedures shall be documented, maintained, and made available to all users who need them.	Does your institution maintain security configuration standards for information systems and applications?	CISO
A12.1.2	Change management	Changes to information processing facilities and systems shall be controlled.	Are changes to information systems tested, authorized, and reported?	CISO
A12.1.3	Segregation of duties	Duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.	Are duties sufficiently segregated to ensure unintentional or unauthorized modification of information is detected?	CISO

A12.1.4	Separation of development, test and operational facilities	Development, test and operational facilities shall be separated to reduce the risks of unauthorized access or changes to the operational system.	Are production systems separated from other stages of the development life cycle?	CISO
A12.2	**Protection against malicious and mobile code**	**To protect the integrity of software and information.**		
A12.2.1	Controls against malicious code	Detection, prevention, and recovery controls to protect against malicious code and appropriate user awareness procedures shall be implemented.	Are methods used to detect, quarantine, and eradicate known malicious code on information systems including workstations, servers, and mobile computing devices?	IT
A12.2.2	Controls against mobile code	Where the use of mobile code is authorized, the configuration shall ensure that the authorized mobile code operates according to a clearly defined security policy, and unauthorized mobile code shall be prevented from executing.	Are methods used to detect and eradicate known malicious code transported by electronic mail, the web, or removable media?	IT
A12.3	**Back-up**	**To maintain the integrity and availability of information and information processing facilities.**		
A12.3.1	Information back-up	Back-up copies of information and software shall be taken and tested regularly in accordance with the agreed backup policy.	Is your data backup process frequency consistent with the	IT

			availability requirements of your organization?	
A12.4	**Monitoring**	**To detect unauthorized information processing activities.**		
A12.4.1	Audit logging	Audit logs recording user activities, exceptions, and information security events shall be produced and kept for an agreed period to assist in future investigations and access control monitoring.	Does your institution regularly review administrative and operative access to audit logs?	IT
A12.4.2	Monitoring system use	Procedures for monitoring use of information processing facilities shall be established and the results of the monitoring activities reviewed regularly.	Are file-integrity monitoring tools used to alert personnel to unauthorized modification of critical system files, configuration files, or content files and to configure the software to perform critical file comparisons at least weekly?	IT
A12.4.3	Protection of log information	Logging facilities and log information shall be protected against tampering and unauthorized access.	Are steps taken to secure log data to prevent unauthorized access and tampering?	IT
A12.4.4	Administrator and operator logs	System administrator and system operator activities shall be logged.	Does your institution have a process for routinely monitoring logs	IT

			to detect unauthorized and anomalous activities?	
A12.4.5	Fault logging	Faults shall be logged, analysed, and appropriate action taken.	Does your institution record your log reviews (recertification/attestation)?	IT
A12.4.6	Clock synchronization	The clocks of all relevant information processing systems within an organization or security domain shall be synchronized with an agreed accurate time source.	Does your institution have a process to ensure synchronization of system clocks with an authoritative source (e.g., via NTP) on a periodic basis commensurate with the potential risks?	IT
A12.5	**Control of operational software**			
A12.5.1	Installation of software on operational systems	Procedures shall be implemented to control the installation of software on operational systems.	Are security-related activities such as hardware configuration changes, software configuration changes, access attempts, and authorization and privilege assignments automatically logged?	CISO
A12.6	**Technical vulnerability management**			

A12.6.1	Management of technical vulnerabilities	Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.		CISO
A12.6.2	Restrictions on software installation	Rules governing the installation of software by users shall be established and implemented.		CISO
A12.7	**Information systems audit considerations**			
A12.7.1	Information systems audit controls	Audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimize disruptions to business processes.	Are file-integrity monitoring tools used to alert personnel to unauthorized modification of critical system files, configuration files, or content files and to configure the software to perform critical file comparisons at least weekly?	CISO
A12.8	**Third party service delivery management**	**To implement and maintain the appropriate level of information security and service delivery in line with third party service delivery agreements.**		

A12.8.1	Service Delivery	It shall be ensured that the security controls, service definitions, and delivery levels included in the third party service delivery agreement are implemented, operated, and maintained by the third party.		CISO
A12.8.2	Monitoring and review of third party services	The services, reports and records provided by the third party shall be regularly monitored and reviewed, and audits shall be carried out regularly.		CISO
A12.8.3	Managing changes to third party services	Changes to the provision of services, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account of the criticality of business systems and processes involved and re-assessment of risks.		CISO
A12.9	**System planning and acceptance**	**To minimize the risk of systems failure.**		
A12.9.1	Capacity management	The use of resources shall be monitored, tuned, and projections made of future capacity requirements to ensure the required system performance.	Are security-related activities such as hardware configuration changes, software configuration changes, access attempts, and authorization and privilege assignments automatically logged?	IT

A12.9.2	System acceptance	Acceptance criteria for new information systems, upgrades, and new versions shall be established and suitable tests of the system's) carried out during development and prior to acceptance.		IT
A13	**Communications Security**			
A13.1	**Network security management**	**To ensure the protection of information in networks and the protection of the supporting infrastructure.**		
A13.1.1	Network controls	Networks shall be adequately managed and controlled, in order to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit.	Are Internet-accessible servers protected by more than one security layer (firewalls, network IDS, host IDS, application IDS)?	IT
A13.1.2	Security of network services	Security features, service levels, and management requirements of all network services shall be identified and included in any network services agreement, whether these services are provided in-house or outsourced.	Does your institution have a segmented network architecture to provide different levels of security based on the information's classification?	IT
A13.2	**Media handling**	**To prevent unauthorized disclosure, modification, removal or destruction of assets, and interruption to business activities.**		

A13.2.1	Management of removable media	There shall be procedures in place for the management of removable media.	Are controls in place to protect, track, and report status of media that has been removed from secure organization sites?	Administration
A13.2.2	Disposal of media	Media shall be disposed of securely and safely when no longer required, using formal procedures.		Administration
A13.2.3	Information handling procedures	Procedures for the handling and storage of information shall be established to protect this information from unauthorized disclosure or misuse.		Administration
A13.2.4	Security of system documentation	System documentation shall be protected against unauthorized access.		IT
A123.3	**Exchange of information/Electronic Transfer**	**To maintain the security of information and software exchanged within an organization and with any external entity.**		
A13.3.1	Information exchange policies and procedures	Formal exchange policies, procedures, and controls shall be in place to protect the exchange of information through the use of all types of communication facilities.		CISO
A13.3.2	Exchange agreements	Agreements shall be established for the exchange of information and software between the organization and external parties.		CISO

A13.3.3	Physical media in transit	Media containing information shall be protected against unauthorized access, misuse or corruption during transportation beyond an organization's physical boundaries.		Administration
A13.3.4	Electronic messaging	Information involved in electronic messaging shall be appropriately protected.	Does your institution have a process for posture checking, such as current antivirus software, firewall enabled, OS patch level, etc., of devices as they connect to your network?	CISO
A13.3.5	Business information systems	Policies and procedures shall be developed and implemented to protect information associated with the interconnection of business information systems.		CISO
A13.4	**Electronic commerce services**	**To ensure the security of electronic commerce services, and their secure use.**		
A13.4.1	Electronic commerce	Information involved in electronic commerce passing over public networks shall be protected from fraudulent activity, contract dispute, and unauthorized disclosure and modification.	Does your institution have a process in place to ensure data related to electronic commerce (e-commerce) traversing public networks is protected from fraudulent activity, unauthorized	IT

			disclosure, or modification?	
A13.4.2	On-line transactions	Information involved in on-line transactions shall be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.		IT
A13.4.3	Publicly available information	The integrity of information being made available on a publicly available system shall be protected to prevent unauthorized modification.		IT
A14	**Information systems acquisition, development and maintenance**			
A14.1	**Security requirements of information systems**	**To ensure that security is an integral part of information systems.**		
A14.1.1	Security requirements analysis and specification	Statements of business requirements for new information systems, or enhancements to existing information systems shall specify the requirements for security controls.	The information security related requirements shall be included in the requirements for new information systems or	CISO

			enhancements to existing information systems.	
A14.1.2	Securing application services on public networks	Information involved in application services passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification.		CISO
A14.1.3	Protecting application services transactions	In Progress Information involved in application service transactions shall be protected to prevent incomplete transmission, misrouting, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.		CISO
A14.2	**Security in development and support processes**	**To maintain the security of application system software and information.**		
A14.2.1	Secure Development Policy	Rules for the development of software and systems shall be established and applied to developments within the organization.		S/W
A14.2.2	System Change control procedures	The implementation of changes shall be controlled by the use of formal change control procedures.		S/W
A14.2.3	Technical review of applications	When operating systems are changed, business critical applications shall be reviewed and tested to ensure there is no		IT

	after operating system changes	adverse impact on organizational operations or security.		
A14.2.4	Restrictions on changes to software packages	Modifications to software packages shall be discouraged, limited to necessary changes, and all changes shall be strictly controlled.		IT
A14.2.5	Secure system engineering principles	Principles for engineering secure systems shall be established, documented, maintained and applied to any information system implementation efforts.		IT
A14.2.6	Secure development environment	Organisations shall establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle.		IT
A14.2.7	Information leakage	Opportunities for information leakage shall be prevented.		IT
A14.2.8	Outsourced software development	Outsourced software development shall be supervised and monitored by the organization.		S/W
A14.2.9	System security testing	Testing of security functionality shall be carried out during development.		S/W
A14.2.10	System acceptance testing	Acceptance testing programs and related criteria shall be established for new information systems, upgrades and new versions.		S/W

A14.2	**Correct processing in applications**	**To prevent errors, loss, unauthorized modification or misuse of information in application.**		
A14.2.1	Input data validation	Data input to applications shall be validated to ensure that this data is correct and appropriate.		S/W
14.2.2	Control of internal processing	Validation checks shall be incorporated into applications to detect any corruption of information through processing errors or deliberate acts.		S/W
14.2.3	Message integrity	Requirements for ensuring authenticity and protecting message integrity in applications shall be identified, and appropriate controls identified and implemented.		S/W
14.2.4	Output data validation	Data output from an application shall be validated to ensure that the processing of stored information is correct and appropriate to the circumstances.		S/W
A14.3	**Security of system files /test Data**	**To ensure the security of system files**		
A14.3.1	Control of operational software	There shall be procedures in place to control the installation of software on operational systems		IT
A14.3.2	Protection of system test data	Test data shall be selected carefully, and protected and controlled.	Test data shall be selected carefully, protected and controlled.	S/W

A14.3.3	Access control to program source code	Access to program source code shall be restricted.		S/W
A14.6	**Technical Vulnerability Management**	**To reduce risks resulting from exploitation of published technical vulnerabilities.**		
A14.6.1	Control of technical vulnerabilities	Timely information about technical vulnerabilities of information systems being used shall be obtained, the organization's exposure to such vulnerabilities evaluated, and appropriate measures taken to address the associated risk.		IT
A15	**Supplier Security**			
A15.1	**Reporting information security events and weaknesses**	**To ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken.**		
A15.1.1	Monitoring and review of supplier services	Does your institution specify security requirements in contracts with external entities (third party) before granting access to sensitive institutional information assets?		Procurement
A15.1.2	Managing changes to supplier services	Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account of the		Procurement

		criticality of business information, systems and processes involved and reassessment of risks.		
A15.1.3	Reporting information security events	Does your institution specify security requirements in contracts with external entities (third party) before granting access to sensitive institutional information assets?		Procurement
A15.1.4	Reporting security weaknesses	Are requirements addressed and remediated prior to granting access to data, assets, and information systems?		Procurement
A15.1.5	Third party service delivery management	Do agreements for external information system services specify appropriate security requirements?		Procurement
		Does your institution have a process in place for assessing that external information system providers comply with appropriate security requirements?		Procurement
		Is external information system services provider compliance with security controls monitored?		Procurement
		Are external information system service agreements executed and routinely reviewed to ensure security requirements are current?		Procurement
A16	**Information security**			

	incident management			
A16.1	**Reporting information security events and weaknesses**	**To ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken.**		
A16.1.1	Responsibilities and procedures	Management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to information security incidents.	Are incident-handling procedures in place to report and respond to security events throughout the incident life cycle, including the definition of roles and responsibilities?	CISO
A16.1.2	Reporting information security events	Information security events shall be reported through appropriate management channels as quickly as possible.	Are incident-handling procedures in place to report and respond to security events throughout the incident life cycle, including the definition of roles and responsibilities?	CISO
A16.1.3	Reporting security weaknesses	All employees, contractors and third party users of information systems and services shall be required to note and report any observed or suspected security weaknesses in systems or services.	Are your incident response staff aware of legal or compliance requirements surrounding evidence collection?	CISO

A16.1.4	Assessment of and decision on information security events	Information security events shall be assessed and it shall be decided if they are to be classified as information security incidents.		CISO
A16.2	**Management of information security incidents and improvements**	**To ensure a consistent and effective approach is applied to the management of information security incidents.**		
A16.2.1	Responsibilities and procedures	Management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to information security incidents.		CISO
A16.2.2	Learning from information security incidents	There shall be mechanisms in place to enable the types, volumes, and costs of information security incidents to be quantified and monitored.		CISO
A16.2.3	Collection of evidence	Where a follow-up action against a person or organization after an information security incident involves legal action (either civil or criminal), evidence shall be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s).		CISO
A17	**Business continuity management**			

A17.1	**Information security aspects of business continuity management**	**To counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.**		
A17.1.1	Business continuity planning framework	A single framework of business continuity plans shall be maintained to ensure all plans are consistent, to consistently address information security requirements, and to identify priorities for testing and maintenance.	The organization shall determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster.	CISO
A17.1.2	Developing and implementing continuity plans including information security	Plans shall be developed and implemented to maintain or restore operations and ensure availability of information at the required level and in the required time scales following interruption to, or failure of, critical business processes.	Does your institution have a documented business continuity plan for information technology that is based on a business impact analysis, is periodically tested, and has been reviewed and approved by senior staff or the board of trustees?	CISO
A17.1.3	Implementing information security continuity	The organization shall establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity		CISO

		for information security during an adverse situation.		
A17.1.4	Including information security in the business continuity management process	A managed process shall be developed and maintained for business continuity throughout the organization that addresses the information security requirements needed for the organization's business continuity.		CISO
A17.1.5	Business continuity and risk analysis	Events that can cause interruptions to business processes shall be identified, along with the probability and impact of such interruptions and their consequences for information security.		CISO
A17.1.6	Testing, maintaining and re-assessing business continuity plans	Business continuity plans shall be tested and updated regularly to ensure that they are up to date and effective.		CISO
A17.1.7	Verify, review and evaluate information security continuity	The organization shall verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations.		CISO
A17.2	**Redundancies**			

A17.2.1	Availability of information processing facilities	Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.		CISO
A18	**Compliance**			
A18.1	**Compliance with legal requirements**	**To avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements.**		
A18.1.1	Identification of applicable legislation and contractual requirements	All relevant statutory, regulatory and contractual requirements and the organization's approach to meet these requirements shall be explicitly defined, documented, and kept up to date for each information system and the organization.	Does your institution have a records management or data governance policy that addresses the life cycle of both paper and electronic records at your institution?	Finance
A18.1.2	Intellectual property rights (IPR)	Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory, and contractual requirements on the use of material in respect of which there may be intellectual property rights and on the use of proprietary software products.	Does your institution have an enforceable data protection policy that covers personally identifiable information (PII)?	IT
A18.1.3	Protection of organizational records	Important records shall be protected from loss, destruction and falsification, in accordance with statutory, regulatory, contractual, and business requirements.		IT
A18.1.4	Data protection and privacy of	Data protection and privacy shall be ensured as required in relevant	Does your institution have an Acceptable Use	Finance

	personal information	legislation, regulations, and, if applicable, contractual clauses.	Policy that defines misuse?	
A18.1.5	Prevention of misuse of information processing facilities	Users shall be deterred from using information processing facilities for unauthorized purposes.		Administration
A18.1.6	Regulation of cryptographic controls	Cryptographic controls shall be used in compliance with all relevant agreements, laws, and regulations.	Does your institution provide guidance for the community on export control laws?	IT
A18.2	**Compliance with security policies and standards, and technical compliance**	**To ensure compliance of systems with organizational security policies and standards**		
A18.2.1	Independent review of information security	The organization's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) shall be reviewed independently at planned intervals or when significant changes occur.	Are standard operating procedures periodically evaluated for compliance with your organization's security policies, standards, and procedures?	Top Management
A18.2.2	Compliance with security policies and standards	Managers shall ensure that all security procedures within their area of responsibility are carried out correctly to achieve compliance with security policies and standards.	Are standard operating procedures periodically evaluated for compliance with your organization's security policies,	Top Management

			standards, and procedures?	
A18.2.3	Technical compliance checking	Information systems shall be regularly checked for compliance with security implementation standards.	Does your institution perform periodic application and network layer vulnerability testing or penetration testing against critical information systems?	IT
A18.3	**Information system audit considerations**	**To maximize the effectiveness of and to minimize interference to/from the information systems audit process.**		
A18.3.1	Information systems audit controls	Audit requirements and activities involving checks on operational systems shall be planned carefully and agreed to minimize the risk of disruptions to business processes.	Are you performing independent audits on information systems to identify strengths and weaknesses?	IT
A18.3.2	Protection of information systems audit tools	Access to information systems audit tools shall be protected to prevent any possible misuse or compromise.	Are audit tools properly separated from development and operational system environments to prevent any misuse or compromise?	IT
Legend				
Count	**Status Code**	**Meaning**		
159	**D**	Control is documented and implemented		

0	**MD**	Control is implemented and process must be documented to ensure repeatability of process and mitigate the risks.		
0	**RD**	Control is not comply with standards and it must be redesigned to comply with standards		
0	**PNP**	Process is not in place / not implemented. (Required Control is neither documented nor implemented)		
0	**NA (Not Applicable)**	Control is not applicable for the company as per the business		
159				