UNIVERSITY OF NAIROBI
SCHOOL OF COMPUTING AND INFORMATICS

AN INFORMATION SECURITY GOVERNANCE FRAMEWORK FOR THE PUBLIC SECTOR IN KENYA

NICHOLAS MULEI MBITHI
P56/61303/2010

SUPERVISOR
MR. DAN ORWA

JUNE 2012

Submitted in partial fulfilment of the requirements for the award of Master of Science Degree in Information Systems

Declaration

I declare that this project work as presented in this report is my own original work and has not been presented anywhere else for any award.

Signature... Date.....27/7/2012..............................

Nicholas Mbithi

P56/61303/2010

This work has been submitted as part of the fulfillment of the requirements for the award of Master of Science in Information Systems degree at the University of Nairobi with my approval as the university supervisor.

Signed... Date.....28/7/12....................................

Mr. Dan Orwa

School of Computing and Informatics

University of Nairobi

Acknowledgements

First and foremost I thank the Almighty God for giving me the strength and will to pursue and accomplish my studies successfully.

Secondly I am highly appreciative of the guidance and support accorded to me by my supervisor Mr. Dan Orwa throughout my research work from the point of selecting the topic of study to the final project report.

Finally to my dear wife Judy and our beloved daughter June whose support and understanding throughout the entire period of my studies for my degree has seen me have a less strenuous study life, I say thank you very much.

Dedication

I happily dedicate this report to my dear wife Judy and my beloved daughter June for the unconditional support they accorded me throughout the period of my research.

ABSTRACT

One of the main assets of any institution, be it a private company or a government institution, is information. This being the case, it is imperative for every institution to institute appropriate measures to ensure security of its information. Many reasons have been cited as contributories to breaches of information security. Among this reasons, one which has become quite salient is lack of information security governance framework for institutions to follow while implementing information security measures.

Therefore, lack of information security governance framework having been identified as one of the main factors that contribute to the slow progress in implementation of information security measures in institutions – including those in public sector – then the study sought to propose an information security governance framework for ensuring security of IT resources in the public sector in Kenya.

In an effort to actualize the study, several objectives that were meant to guide in carrying out our research were.

To determine the effectiveness with which the public sector in Kenya is currently addressing the challenge of information security, to identify security challenges facing the public sector in Kenya, to identify the members of staff responsible for information security in public institutions in Kenya and to propose a framework for adoption in the public sector in Kenya for information security governance.

To achieve the said objectives, the study used survey design as the research methodology, in which information was gathered through administration of questionnaires to a sample of respondents from public institution in Kenya. The institutions were drawn from the three main categories of institutions in the public sector i.e. Central Government, Local Government and State Corporations.

For data analysis, SPSS statistical software version 16.0 was utilized. During data analysis there emerged some issues worth noting.

In conclusion, the study demonstrated how each of the outlined objectives of the study was achieved. Further, recommendations were given for further study especially where it was recommended that a study need to be carried out to shed more light into the fact that in most of the institutions, it is the Unit Heads who are responsible for most of information security roles.

TABLE OF CONTENTS

List of Tables

List of Figures

List of Abbreviations

i. CEO – Chief Executive Officer
ii. CIO - Chief Information Officer
iii. CISO - Chief Information Security Officer
iv. EDI - Electronic Data Interchange
v. ICT - Information and Communication Technologies
vi. IM - Instant Messaging
vii. IS - Information System
viii. ISO/IEC - International Organization for Standardization / International Electro-technical Commission
ix. IT - Information Technology
x. PC - Personal Computer
xi. PDA - Personal Digital Assistant
xii. USA – United States of America

CHAPTER ONE: INTRODUCTION

1.1. Background

One of the most important assets in an organization is Information, its security is of great significance and efforts need to be instituted to secure it at all times.

One of the main reasons for information security, as observed by Fielden (2011), is economic protection; organizations would want to make sure that their economic wellbeing is not compromised by lack of proper information security.

Besides the need for sound technological measures in protecting ICT resources, organizations need also to ensure that there are sound policies, procedures and standards to augment technology. This does not only ensure security of ICT resources but also ensures compliance to the Law and Regulations.

Any organization would want to ensure that confidentiality and integrity of its information is assured and also ensuring that the two aspects do not impact negatively on the availability of the organization's information resource to the authorized persons; hence this calls for a balance to be struck between the two virtues and information availability to the intended persons.

To assure sound information security, there is a need for this aspect to be viewed from the security of all those components that make up ICT resources; all hardware, software, data, information, network, personal computing devices, support personnel, and users. The hardware need to be protected from unauthorized access. Further, if an individual has been authorized to access the hardware housing information, then he/she should only be able to access those applications which they have been authorized to access. These security measures need also to be implemented for the organizations network resources; an individual's rights to access the organizations network resources should be controlled to ensure security of the information transmitting through the network.

In today's business operations, the internet has become very important for many reasons. Fielden (2011) notes that, the internet has outgrown its original purpose and role and so has information security. He notes that there are important aspects that the internet has enabled and consequently called for reviewed information security importance. Some of these areas of security concern are:

i. Economic protection – economic protection is required in different levels i.e. globally, nationally, commercially, educationally and also at individual level. A secure internet provides opportunities for wealth based on secure information.

ii. E-governance – information security and privacy are real concerns for e-government technologies. If a nation has concern over security and terrorism and has its citizen's privacy and civil liberty spelled out in its culture, then there is need of a comprehensive national cyber-security strategy which encompasses both intelligence and law enforcement.

iii. Human rights – the internet has irrevocably changed how information is distributed globally. This has impacted on human rights in that, the internet has amplified opinions and interests, accelerated and freed dissemination of information and enabled faster delivery of services.

To assure sound and optimum security measures for ICT resources, an organization will need to have a good information security governance framework in place. The framework will provide broad based security measures which act as a skeleton on which more elaborate and detailed measures are developed. According to Kimwele et al (2011) IT security is often taken as a technology issue, leaving the more important governance perspective of IT security. In their publication Kimwele et al (2011) observes "Looking at the growing abundance of rules, regulations, and guidelines, it is clear that information security is not solely a technical issue, but also a corporate governance challenge". This view is further emphasized by Casmir (2005) when he observes that information systems fail not entirely because of technology issues or technical competence of the people administering them, but also because of lack of awareness to the end users.

1.2. Problem Statement

As more and more organizations embrace information technology in their day to day operations, there is a need to assure the security of the information and also the infrastructure through which the information is made available; making up IT resources. Efforts directed towards information security, policies developed with information security in mind, and regulations requiring specific types of information security activities in specific industries could possibly all contribute to the assurance of the security of the IT resources Ryan (2001).

The government of Kenya partnering with the private sector has invested in fiber optic cable with the first cable – TEAMS – landing in Kenya in June 2009.This investment has greatly improved access to the internet by both government and private institutions. This increased rate of internet connectivity by government institutions brings with it related security threats. As Sipior and Ward (2008) notes, the use of internet has brought with it escalation of concerns which include consumer confidence in online business activities, threats to data integrity, legal liability not to mention the possibility of suffering financial loss. In the Kenyan situation, a related case in the recent past is the hacking into the Kenyan Police website.

According to Corner et al (2003), despite there being many solutions that have been proposed, technologies which have been proven and readily available and the consequences of inaction becoming clearer every day, lack of information security framework is one of the main reasons that stand in the way of making significant progress in information security. According to Gupta & Sharman (2008) people tend to be the most likely to be exploited link in information security implementation hence there is a need for a framework to guide individuals on their respective roles to ensure information security.

Therefore, lack of information security governance framework having been identified as one of the main factors that contribute to the slow progress in implementation of information security measures in institutions – including those in public sector – then the study sought to propose an information security governance framework for ensuring security of IT resources in the public sector in Kenya.

1.3. Justification of the Study

Institutions rely on information in their day-to-day operations. This has not been any different for institutions in the public sector. As more reliance is placed in information systems, the institutions are reaping more benefits and opportunities that come with information technology. However, it is not only the benefits and opportunities that are brought by information technology that institutions are enjoying, but they also have to content with challenges that are associated with it. Some of the security challenges faced are denial of service attacks, intrusions by computer hackers, malicious software e.g. viruses and Trojan horses.

It is these challenges of security that are posed by implementation of information systems, that this project wanted to address; more so in the public sector in Kenya.

Therefore the study intended to provide public institutions in Kenya with a framework that they can adopt in addressing the challenges of information security governance. This is because, the framework will be designed to be easy to implement and to a large extent address information security challenges these institutions face.

The study addresses itself to several key audiences.

i. For the public sector institutions in Kenya the research contributes towards addressing their security challenges, by proposing a framework for implementation of information security governance measures.
ii. For security agencies, the research provides a means for evaluating institutions information security preparedness. Therefore, the agencies will be in a better position to carry out audits of information security.
iii. For the general public the study assures them that information which has been entrusted with public institutions, for example with the ministry of immigration and registration of persons, is safe from possible threats, because these institutions have implemented information security measures.

1.4. Research Objectives

i. To determine the effectiveness with which the public sector in Kenya is currently addressing the challenge of information security
ii. To identify security challenges facing the public sector in Kenya.
iii. To identify those responsible for information security in public institutions in Kenya.
iv. To explore frameworks on information security and adopt one that can be used by the public sector in Kenya to address the challenges of information security governance. This would assure the integrity, availability and also confidentiality of the information.
v. To evaluate the effectiveness of the framework proposed.

1.5. Research Questions

i. How effective are public institutions in Kenya addressing information security challenges?

ii. What are the information security threats faced by public institutions in Kenya while implementing information security measures?

1.6. Assumptions of the Research

The following are the assumptions of the study.

i. It was assumed that the respondents to any of the research tools used will be truthful and knowledgeable enough to field questions posed.

ii. It was further assumed that the framework would be readily embraced by the users, i.e. institutions in the public sector.

iii. All sampled institutions would participate in the study.

1.7. Chapter Summaries

Chapter one on introduction, different areas were discussed. After background information of the study, the problem being addressed – lack of a framework for information security – was outlined. Project justification and project main objectives were also discussed. Before the chapter was concluded, limitations and assumptions of the study were mentioned.

In chapter two, which is on literature review, other scholarly works and other relevant sources of previous works on the area of information security were reviewed. A comprehensive framework by Conner et al (2003) was been reviewed where their findings on information security issues were highlighted. Also, ISO/IEC 27002:2005 standard on information security is discussed and its outline given. A sample information security framework from State of Indiana in the USA was highlighted. IT security framework for SMEs in Kenya by Kimwele et al (2011) was finally discussed.

To conclude the chapter, a theoretical framework Conner et al (2003) was chosen for replication in the Kenyan scenario.

The third chapter is on research methodology. In the chapter survey design was identified as the research methodology, in which information was gathered through administration of questionnaires to a sample of respondents from public institution in Kenya. The institutions were drawn from the three main categories of institutions in the public sector i.e. Central Government, Local Government and State Corporations.

The fourth chapter is on Results and Discussion. This this chapter, the data collected is analyzed using analysis methodology and tools identified in the third chapter on research methodology.

The last chapter of the study is on conclusion and recommendations. In the chapter the achievements of the study are demonstrated by showing how the objectives of the study were achieved. Any limitations and recommendations for further study are given.

CHAPTER TWO: LITERATURE REVIEW

2.0. Introduction

According to Kombo and Tromp (2006), literature review gives an account of what has already been published on a topic by other researchers. In light of this, several previous works, relevant to the area of our research were reviewed so as to appreciate what other scholars had been able to do in the same field. There are those works which were considered to be more relevant to the field of our study and they are discussed below. A theoretical framework used during the study is included at the end of the chapter.

2.1. ISO/IEC 27002:2005 Information Technology – Security Techniques – Code of Practice for Information Security Management

ISO and IEC are the two bodies that form the specialized system for worldwide standardization. ISO/IEC 27002:2005 the latest version of the ISO standard "Information technology – security techniques – Code of practice for information security management", is an internationally accepted standard of good practice for information security. Thousands of organizations worldwide are said to follow the standard.

The standard was previously known as ISO/IEC 17799:2005 before year 2007. In June 2005, the 2000 version of the standard had significant updates with new sections consolidating advice on risk and incident management. The format was also altered so as to clarify the 'implementation guidance' under each control.

The standard establishes guidelines and general principles for initiating, implementing, maintaining and improving information security management in an organization. The standard may serve as a practical guideline for developing organizational security standards and effective security management practices and to help build confidence in inter-organizational activities.

The standard is explicitly concerned with information security, meaning the security of information assets and not just IT systems. Even though the IT Department in any organization is usually viewed as the custodian of a sizeable proportion of the organization's information assets, it is not necessarily the ideal home for the information security management function.

2.1.1. Information Security

According to the (ISO/IEC 27002:2005), information security is the protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investment and business opportunities.

It is further noted that, information security is achieved by implementing a suitable set of controls that consist of policies, processes, procedures, organizational structures and software and hardware functions. The mentioned controls will need to be established, implemented, monitored, reviewed and improved to ensure that the particular security and business objectives of the organization are met. This exercise should not be done in isolation but in conjunction with other business management processes.

2.1.2. Need for Information Security

Information together with the supporting processes, systems and networks are crucial business assets. If a business is to maintain a competitive edge, cash flow, its profitability, legal compliance and also its commercial image, then security of its information asset is critical.

Organizations are more and more faced with increasing number of threats which may include computer-assisted fraud, espionage, sabotage, vandalism, fire not to mention floods. Other threats would be like malicious code, computer hackers and denial of service attacks.

Information security is not only important to the private sector but also in the public sector as well. In both sectors, information security takes the role of an enabler, for instance in enabling e-government or e-business and averting the likely risks. There is increased interconnection of public and private networks and sharing of information resources which has not helped in security because the aspect of access control becomes more challenging. Furthermore distributed computing is a trend which is catching up fast a phenomenon which further complicates matters with information security; this is because the effectiveness of central, specialist control is weakened.

Though there are concerted efforts towards technical means in implementing information security, it has been found that technical means do not work well by themselves; hence there is a need for the technical means to be supported by appropriate management and procedures. Information security management will require at least participation of all employees in the organization. Further participation from other stakeholders may be called for to come up with sound security controls, these stakeholders could be shareholders, suppliers, customers and other external parties.

2.1.3. Establishing Security Requirements

The standard identifies three main areas from which security requirements may be sourced.

i. Through risk assessment – By carrying out risk assessment, threats to assets are identified, vulnerabilities and likelihood of occurrence are evaluated and potential impact of the threats is estimated.

ii. Every organization has legal, statutory, regulatory, and contractual requirements with its trading partners, contractors and service providers; this is a another source of security requirements.

iii. Finally the standard identifies the organization's particular principles, objectives and business requirements for information processing that it has developed to support its operations, as another source of security requirements.

2.1.4. Assessing Security Risks

This is one of the main ways of identifying security requirements. Methodical assessment of security risks would help in security requirements identification. This assessment helps organizations to come up with controls in relation to the likely business harm from security failures. This exercise of risk assessment should be carried out periodically to address changes that might impact on the risk assessment results.

2.1.5. Implementing Information Security

There are a number of controls that can be considered as a good starting point for implementing information security. These controls are either based on essential legislative requirements or considered to be common practice for information security.

1. **Controls considered to be essential to an organization from a legislative point of view include the following:**

a. Data protection and privacy of personal information
b. Protection of organizational records.
c. Intellectual property rights.

2. **Controls considered being common practice for information security will include:**

a. Information security policy document
b. Allocation of information security responsibilities.
c. Information security awareness, education and training
d. Correct processing in applications
e. Technical vulnerability management
f. Business continuity management
g. Management of information security incidents and improvements.

The above controls apply to most organizations and in most environments.

2.1.6. Critical Success Factors

The standard notes that there are factors which experience has shown would be critical to the success of any information security implementation in an organization.

a. information security policy, objectives, and activities that reflect business objectives;
b. an approach and framework to implementing, maintaining, monitoring, and improving information security that is consistent with the organizational culture;
c. visible support and commitment from all levels of management;
d. a good understanding of the information security requirements, risk assessment, and risk management;
e. effective marketing of information security to all managers, employees, and other parties to achieve awareness;
f. distribution of guidance on information security policy and standards to all managers, employees and other parties;
g. provision to fund information security management activities;

h. providing appropriate awareness, training, and education;
i. establishing an effective information security incident management process;
j. Implementation of a measurement system that is used to evaluate performance in information security management and feedback suggestions for improvement.

2.1.7. Structure and format of the standard

ISO/IEC 27002 is a code of practice i.e. it is an advisory document and not formal specification for information security. It lays out a structured set of suggested controls to mitigate information security risks, covering confidentiality, integrity and availability aspects. If an organization opts to adopt the standard in addressing its information security issues, then it needs to first assess its information security risks and then apply suitable controls, using the standard for guidance. Even though it is not a must to implement all the controls stipulated in the standard, an organization which fails to implement one of them, then it needs to demonstrate it was through risk assessment that it was found not to be necessary to implement it and not because of an oversight of the control; this is necessary if the organization wants to be certified.

2.1.8. Control Objectives

The standard specifies thirty nine (39) control objectives to protect information assets against threats to their confidentiality, integrity and availability. These control objectives in essence define functional requirements specification for an organization's information security management architecture.

The control objectives make a viable starting point in defining broad based principles for information security policies by just implementing minimum adjustments.

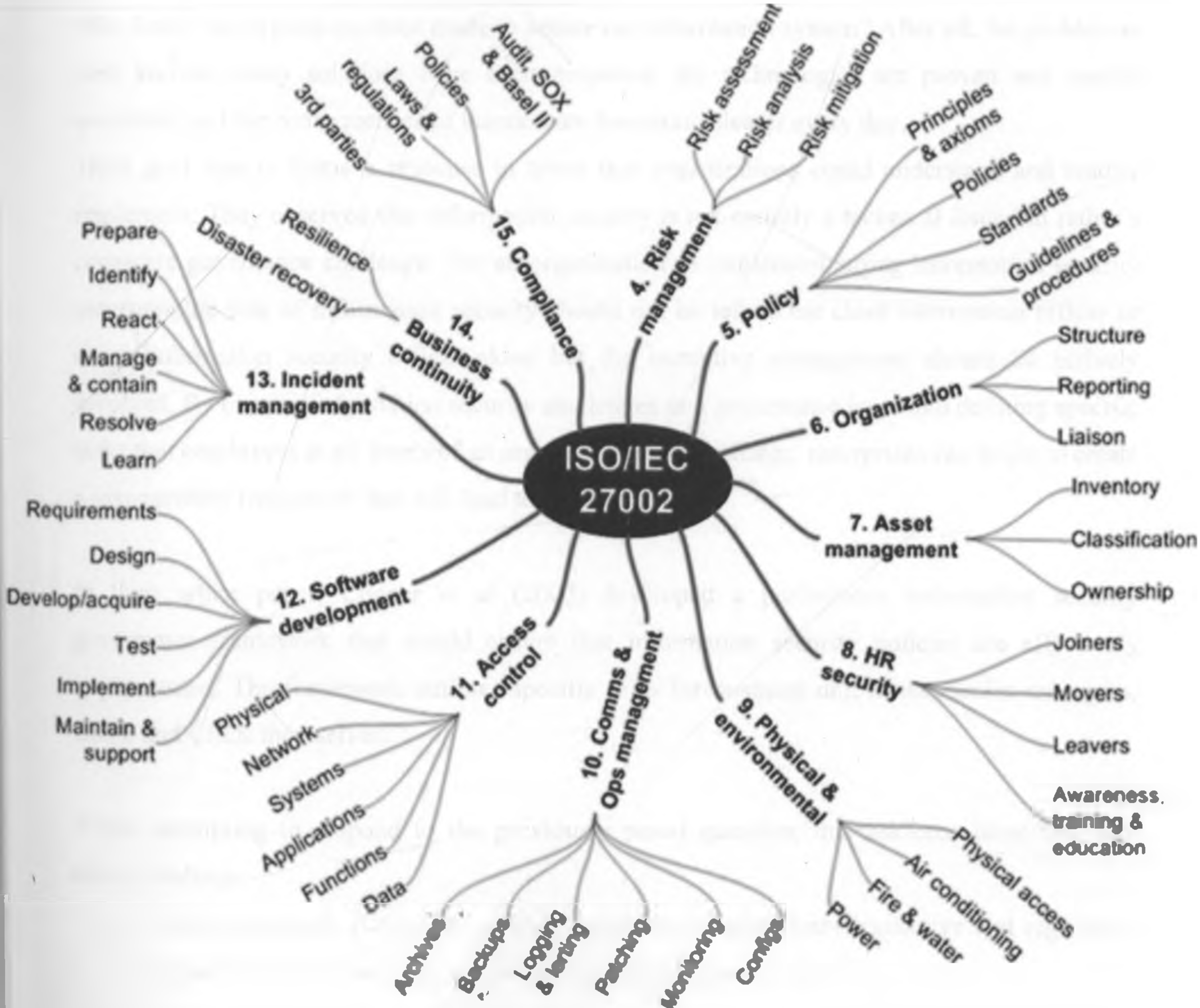
2.1.9. Information Security Specific Controls

The standard addresses itself to a large number of best-practice information security control measures that an organization would consider to meet the control objectives. The standard leaves organizations to choose for them, those control measures that would appropriately suite to their situation given a risk assessment exercise. Organizations are not limited to control measures stated in the standard but can also implement their own control measures if they help to meet the control objectives.

2.1.10. Contents of ISO/IEC 27002 (outline)

The mind map summarizes the main sections of the standard on one side. The sections are outlined below.

Figure 1: Contents of ISO/IEC 27002 mind map



Source: Retrieved from – http://www.iso27001security.com/html/27002.html#Section13 on 22 Jul 2011

The standard covers in detail the operational aspects of information security. However, it does not address effectively the more strategic aspect of information security i.e. information security governance.

2.2. Information Security Governance: Towards a Framework for Action

Conner et al (2003), who were members of Information Security Governance Task Force formed by the Business Software Alliance, were tasked with finding an answer to the following question:

Why hasn't more progress been made to secure our information system? After all, the problem is well known; many solutions have been proposed; the technologies are proven and readily available; and the consequences of inaction are becoming clearer every day.

Their goal was to frame a response in terms that organizations could understand and readily implement. They observed that information security is not entirely a technical issue but rather a corporate governance challenge. For an organization to implement strong information security measures the role of information security should not be left to the chief information officer or chief information security officer alone but the executive management should be actively involved. By treating information security challenges as a governance issue and defining specific tasks that employees at all levels of an organization can discharge, enterprises can begin to create a management framework that will lead to positive results.

In their white paper, Conner et al (2003) developed a preliminary information security governance framework that would ensure that information security policies are effectively implemented. The framework outlines specific roles for business unit heads, senior managers, CIOs, and CEOs themselves.

While attempting to respond to the previously posed question, the taskforce identified four salient findings.

i. The Government (USA) has already established a significant legislative and regulatory regime around IT security, and is considering additional action.

ii. Information security is often treated solely as technology issue, when it should also be treated as governance issue.

iii. There is already broad consensus on the actions necessary to remedy the problem.

iv. Lack of progress is due in part to the absence of a governance framework. If progress is to be accelerated, a management framework that instructs personnel at different levels about how to implement solutions is crucial.

To address the fourth finding, the task force developed a preliminary governance framework, for comment and refinement by both public and private organizations. A summary of the framework is provided below.

Table 1: Preliminary Governance Framework

Actors/Actions	**Corporate Executives**	**Business Unit Heads**	**Senior Manager**	**CIO/CISO**
Governance/Business Drivers	What am I required to do? What am I afraid not to do?			
Roles and Responsibilities	How do I accomplish my objectives			
Metrics/Audit	How effectively do I achieve my objectives? What adjustments do I need to make?			

Source: Adapted from Conner et al (2003)

The preliminary governance framework above poses three sets of questions in respect of information security:

1. What am I required to do? / What am I afraid not to do
2. How do I accomplish my objectives?
3. How effectively do I achieve my objectives? / What adjustments do I need to make?

At each level of management as shown in the preliminary governance framework i.e. Corporate Executives, Business Unit Heads, Senior Managers and CIO/CISO different answers to the questions are likely to be provided, but all will be geared towards an effective and concerted effort towards information security.

The first set of questions defines business drivers that drive business objectives e.g. adherence to regulation could be the driver for CEO. The second question addresses the programs and processes that need to be put in place to accomplish information security objectives. The last set of questions addresses the aspect of measuring effectiveness of security controls and assessing risks through use of appropriate metrics and audit.

Each of the different players in information security governance will tend to afford different importance to information systems whether in the dimension of roles or matrix for evaluation Myers et al (1997).

2.2.1. Four Findings the Task Force

1) Government has already established a significant legislative and regulatory regime around IT security, and is considering additional action.

Even though there is a heightened awareness of the importance of security, many factors have contributed to the perception that progress has been slow. For example, the cost of security is not cheap and demonstrating return on security investment is sometimes difficult. The good news is that industry and government are actively engaged in addressing the information security challenge. Besides the industry, the government through legislature has taken action to address the information security challenge. Conner et al (2003) observed that there were examples of legislation which has been developed to address the challenge. This legislation is mostly United States based;

- Public Company Accounting Reform and Investor Protection Act (also known as Sarbanes-Oxley). It requires firms to certify the integrity of their financial records, their information disclosure controls and internal controls. For this certification to be done there needs to be a serious attention to electronic information security.
- Health Insurance Portability and Accountability Act of 1996 (HIPAA), for protecting health information of individuals.
- Database Security Breach Notification Act, which is a law passed in the state of California, requires companies to notify customers if they believe a systems breach has led to the release of their personal information. A case in mind would be the security breach in the SONY

PlayStation in which the company's systems were hacked into and a lot of customers' personal data made public.

2) **Information security is often treated solely as technology issue, when it should also be treated as governance issue.**

The above finding has also been noted by Casmir (2005) when he observes that information systems fail not entirely because of technology issues or technical competence of the people administering them, but also because of lack of awareness to the end users.

Within many organizations, there are two important barriers to effective computer security:

i. Responsibility is too often delegated to the chief information officer or the chief information security officer who may not be in a position to leverage resources and authority necessary to address the problem of across multiple business lines or divisions. Because usually little attention is given to the issue of information security at the CEO level, then information security efforts are usually underfunded in proportion to the risk and magnitude of harm that incidents could cause.

ii. The second one is lack of a framework for action. A framework would be used to set priorities, assign tasks, get started and monitor implementation. To aid organizations in attacking the problem, numerous guides have been developed. However, there is no recognized standard approach. Without such an approach firms are unclear how to allocate information security funding and energy and how to measure the return on investment.

3) **There is already broad consensus on the actions necessary to remedy the problem**

- There is a broad consensus among the experts as to what kinds of measures should be undertaken by organizations.
- No particular document provides the necessary governance framework for information security. The existing guidance is either too detailed or not actionable in a comprehensive manner from the top to bottom of an organization.

- ISO/IEC 17799 and FISMA (Federal Information Security Management Act) provide a good substantive basis for creating such a framework. However ISO 17799 is overly detailed whereas FISMA is too detailed and government specific to be applied uniformly across all organizations.

In their proposal Conner et al (2003) noted the ISO standard as being used as the baseline reference for the people-operational, people-tactical, process-operational, process-tactical, technology-operational, technology-tactical, technology-strategic dimensions of the matrix. However the ISO standard is very detailed at the operation level yet vague about senior management responsibilities.

FISMA contains high-level management guidance that assigns responsibility at appropriate levels for specific aspects of an organization's information security program. Therefore FISMA is used as the baseline reference for the people-strategic and process-strategic dimensions of the matrix. It provides a useful benchmark at the strategic level.

Eventually Conner et al (2003) came up with a three by three matrix to depict the analysis. The matrix has dimensions of people-process-technology and operational-tactical-strategic. The people-process-technology side refers to people (who), process (how), and technology (what). The operational-tactical-strategic side of the matrix refers to the extent of the strategic nature of recommendations: operational (daily), tactical (review/follow-up), and strategic (annual reviews, establishing policies, organizational view).

Table 2: IT Security Governance Document Analysis

	Operational	Tactical	Strategic
People	Ref = ISO 17799	Ref = ISO 17799	Ref = FISMA
Process	Ref = ISO 17799	Ref = ISO 17799	Ref = FISMA
Technology	Ref = ISO 17799	Ref = ISO 17799	Ref = ISO 17799

Source: Adapted from Corner et al (2003)

4) Lack of progress is due in part to the absence of a governance framework.

The taskforce concluded that a vital piece to solve the puzzle of there being lack of progress in information security governance was information security governance framework that private industry can readily adopt. Governance operationalizes the information security effort.

By themselves, recommended practices – no matter how strong the consensus is for them – are not enough; they must be married with an information security governance framework that assures effective implementation.

2.2.2. Purpose of a Governance Framework

A governance framework is important because it provides a roadmap for the implementation, evaluation and improvement of information security practices, Conner et al (2003).

One of the most important features of a governance framework is that it defines the roles of different members of an organization. This allows organizations to assign specific tasks and responsibilities.

2.2.3. Components of a Security Governance Framework

According to Conner et al (2003), FISMA specifies core components required in a security program, as do many other documents, including ISO/IEC 17799. However what is needed is a framework that specifies what corporate executives, business unit heads, senior managers and CIOs/CISOs should do; that identifies business drivers, clarifies roles and responsibilities, recognizes commonalities and defines metrics; and that is flexible enough to apply to different business models.

The taskforce provided the beginnings of such a framework. The horizontal axis of the chart identifies management levels. The vertical axis identifies the business drivers, responsibilities and metrics. It is worth noting that the first and third criteria on the vertical axis (Governance/Business Drivers and Metrics/Audit) are specific to individual businesses and will change according to individual business and industry needs.

Table 3: Preliminary Information Security Governance Framework

Actors\Actions	Corporate Executives	Business Unit Head	Senior Manager	CIO/CISO
Governance/Business Drivers These tend to be sector or Organization-specific.)	**What am I required to do? / What am I afraid not to do?**			
	Legislation, ROI	Standards, policies, budgets	Standards, audit results	Security policies, security operations, and resources
Roles and Responsibilities (These tend to be generic across industries and Organizations.)	**How do I accomplish my objectives?**			
	• Oversight and coordination of policies • Oversight of business unit compliance • Compliance reporting • Actions to enforce accountability	• Provide information security protection commensurate with the risk and business impact. • Provide security training • Develop the controls environment and activities • Report on effectiveness of policies, procedures and practices	• Provide security for information and systems • Periodic assessments of assets and their associated risks • Determine level of security appropriate • Implement policies and procedures to cost effectively reduce risk to acceptable levels • Periodic test of security and controls	• Develop, maintain, and ensure compliance to program • Designate security officer with primary duties and training • Develop required policies to support security program and business unit specific needs • Develop information use and categorization plan • Assist senior managers with their security responsibilities • Conduct security awareness
	How effectively do I achieve my objectives? What adjustments do I need to make?			
Metrics/Audit (These tend to be sector or Organization-specific.)	Financial reporting, monetizing losses, conforming to policies	Policy violations, misuse of assets, internal control violations	Risk assessment and impact analysis, control environment activities, remedial actions, policy and procedure compliance, security and control test results	Security awareness effectiveness, incident response and impact analysis, security program effectiveness, information integrity, effects on information processing

Source: Adapted from Corner et al (2003)

The framework above was designed to be a tool to guide and encourage senior level managers to adopt corporate best practices for security. The framework represents a two-fold benefit to those organizations that adopt it. First, it identifies cornerstone security practices that nearly all organizations are following. Second, it makes recommendations about where in the organization the responsibility best fits so that the integration of those practices evolves into a corporate climate of security. The framework poses three sets of questions, with regard to information security.

1. What am I required to do? /What am I afraid not to do?
2. How do I accomplish my objectives?
3. How effectively do I achieve my objectives? /What adjustments do I need to make?

2.2.4. Consistency with Key Security Practices

The paper cites four main information security requirements:

1. The need for risk assessments. Risks must be understood and acknowledged, and the security measures that are taken must be commensurate with these risks.
2. The need for a security organizational structure.
3. The need to create, communicates, implement, endorse, monitor and enforce security policies across an organization.
4. The need to make every member of the organization aware of the importance of security and to train them in good security practices.

Further, four other recommended practices were cited.

1. The need for access controls to make certain only identified and authorized users with a legitimate need can access information and system resources.
2. The need to consider security throughout the system life cycle.
3. The need to monitor, audit, and review system activity in a routine and regular function.
4. The need for business continuity plans that are tested regularly.

Conner et al (2003) work addresses the challenges of information security by proposing a framework for information security governance. However, the research that led to the development of the framework was based in the USA. Therefore, unless a testing of the framework is carried out in the Kenyan scenario, then its appropriateness may not be vouched.

2.3. Information Security Framework: State of Indiana Information Resources Policy and Practices-Indiana Office of Technology

2.3.1. Overview of the Framework

This is an information security framework that was developed by the state of Indiana Office of Technology to establish security policy and practices for the Indiana State government. The security framework follows mostly the recommendations stipulated in ISO/IEC 27002:2005 standard. Policies are said to provide general, overarching guidance on matters affecting security that State workforce members are expected to follow. Practices document methods and minimum compliance activities as appropriate to ensure that policy objectives are met.

The information security framework is divided into twelve chapters conforming to the areas identified by the ISO standard as areas which need to be addressed when defining an information security platform.

The following are the chapters identified in the State of Indiana information Security Framework.

1. Security Policy – This addresses the scope of policy as well as roles and responsibilities.
2. Organizational Security – focuses more on security responsibilities of the workforce, third parties and outsourcers.
3. Risk Assessment and Treatment – Documents the process taken by the state to identify and assess risk as well as treat the risk through controls and practices.
4. Asset Classification – provides appropriate security to state physical assets
5. Human Resources Security – addresses the considerations with state workforce members prior to employment, during employment, and after termination
6. Physical and Environmental Security – deals with the protection of physical areas and equipment from physical threats and unauthorized access.
7. Communications and Operations Management – The many facets of information technology are addressed here
8. System Access Controls – Here is where access restrictions for users at network, operating system, application and mobile computing levels are set.
9. System Development and Maintenance – Deals with aspects of application development and maintenance security concerns.

10. Information Security Incidents – addresses what need to be done in the event of a security incident
11. Business Continuity – focuses on plans for interruptions of state of Indiana business activities.
12. Compliance – this chapter deals with how the state would comply with laws and statutes, security policies, controls and practices as well as audit considerations.

Under each of the chapters, the framework identifies objectives that need to be met. For each objective a policy is defined, the purpose it serves is stated, a revision date for the policy is given, those persons, groups or systems affected are enumerated and any procedures, compliances & references are stated.

It is important to note here that information security policy framework implementation may vary from one organization to another. Most organizations will develop their information security policies from established models like the ISO/IEC 27002: to address their security requirements. A number of companies may implement an entire information security policy framework that will incorporate various security components cutting across the company establishment. A majority of other organizations would prefer having a number of information security policy frameworks for different sections or business processes.

The sample framework from the state of Indiana in the USA follows the ISO/IEC 27002:2005 standard.

Conner et al (2003), observes that, the standard is majorly concerned with operational and tactical aspects of information security, thereby leaving the more important facet of information security governance which is more strategic in nature.

The framework is also based in the USA hence its appropriateness in Kenyan scenario cannot be vouched for.

2.4. Information Technology (IT) Security Framework for Kenyan: Small and Medium Enterprises (SMEs)

The paper primarily discusses IT security requirements and appropriate metrics for evaluating effectiveness of security measures implemented in the SME sector in Kenya. The main purpose of the study, Kimwele et al (2011), wanted to come up with a framework which among other things would provide some metrics of evaluating the effectiveness of implemented security measures.

It is noted (in the study) that IT security is usually treated solely as a technology issue, when in reality it should be also be treated as a governance issue. These sentiments are the same echoed by Werlinger et al (2009) in which they observe that technological factors are not the only key to the effectiveness of information security controls; but there is also a need to understand the significance of human and organizational factors.

In their study, Kimwele et al (2011) it is observed that there lacked a framework for action within SMEs which would guide in setting priorities, assignment of tasks, getting started and monitoring of IT security measures. This observation concurs with Corner et al (2003) in which it was noted that lack of information security governance framework is one of main impediments in implementation of information security measures.

Kimwele et al (2011) framework was supposed to meet the following objectives.

- Specify what roles owners of SMEs have in reference to IT security
- Provide some metrics that would be used in measurement of the effectiveness of IT security enhancing mechanisms in SMEs
- To provide guidelines on implementation of IT Security for SMEs in Kenya

IT security requirements and metrics

Just as it has been noted by several other studies and standards like ISO/IEC 27002:2005 and in Tarimo (2006), Kimwele et al (2011) has noted several requirements needed for IT security.

i. The need for risk assessments. Risks must be understood and acknowledged and the IT security measures that are taken must be commensurate with these risks.
ii. The need for an IT security organizational culture.

iii. The needs to create, communicate, implement, endorse, monitor, and enforce security policies across an organization.

iv. The need to make every member of the organization aware of the importance of IT security and to train them in good IT security practices.

v. The need for access controls to make certain only identified and authorized users with a legitimate need access information and system resources.

vi. The need to monitor, audit, and review IT security measures regularly.

vii. The need for business continuity plans that are tested regularly.

After data analysis, salient deductions were drawn. The following was identified by the SMEs as aspects that need to be incorporated in a security enhancing mechanism.

i. Create more awareness programs amongst SMEs and offer them related products to help in protection

ii. Education on the topic of internet security

iii. Hold vulnerability seminars to try and show SMEs what goes wrong in their day to day operations.

IT Security Framework for SMEs

The study's recommended framework consisted of the following:

i. Mapping of identified IT security metrics and the IT security issues/activities/aspects the metrics can measure

ii. An approach that can be used to address IT Security issues which deals with continual improvement and establishment of new measures should the implemented ones at any one particular time appear ineffective.

iii. An illustration of how the approach can be utilized in an IT security enhancing mechanism for SMEs. The illustration was done using data collected during the study.

Table 4: Mapping of IT Security Metrics and the IT Security Issues

	IT SECURITY METRICS									
IT CONTROL ISSUES/ACTIVITIES/ASPECTS	Number of reported security incidents	Number of viruses or other malicious code outbreak	Number of comments on the IT security measures in place	Number of cases for use of pirated software	Traffic to unethical websites	Number of virus problems resulting from opening unexpected email attachments	Number of malicious codes resulting from downloading contents from	Adherence to back up routines and procedures	Frequency of IT equipment failure	Reported cases of compliance to IT security standards
Security Policy (Is our IT security policy effective?)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Organizational security (Is there a Director or equivalent member of staff responsible for IT security?)			✓						✓	✓
Asset Control (Can all assets including hardware and software used for information security handling be identified and located?)								✓		
Personnel Security (Are Staff aware that security incidents should be reported to management immediately?)	✓	✓	✓							
Physical and Environmental Security (Is there appropriate physical and environmental security procedures in place to prevent interference with business premises and IT systems?)			✓						✓	
Communications and Operations Management (Are we confident that our anti-virus systems are up to date, and in the event of a virus outbreak, we should be able to protect our systems?)	✓	✓				✓	✓			✓
Access Control (Can users logon/gain access to our systems without being formally registered with their own user account?)			✓							✓
System Development and Maintenance (Can our systems provide audit trails so that usage of the system and data input/changes can be audited?)		✓			✓		✓			✓
Business Continuity Management (Have our security measures been reviewed within the last year?)								✓		✓
Compliance (Is our organization aware that there are established, international IT security standards available for adoption?)	✓									✓

Source: Adapted from Kimwele et al (2011)

Kimwele et al (2011) came up with a comprehensive framework for information security in SMEs in Kenya. As already noted, however, the framework was primarily developed for SMEs. The authors defined SMEs as institutions which had less than 100 permanent employees. Bearing this definition in mind, then most institutions in the public sector will not fall under the ambit of SMEs.

Another notable point is that the framework addresses enterprises in the private sector and not public sector.

2.5. Theoretical Framework

After a review of literature on information security by other scholars, the one on "Information Security Governance: Towards a Framework for Action" by Conner et al (2003) was chosen for replication in the Kenyan public sector.

The research sought to assess the applicability of the said framework in the Kenyan public institutions scenario; in the aim of addressing information security challenges being faced by Kenyan public sector institutions.

The major reason the framework was considered is because it addresses most of the facets highlighted by other frameworks. It does not only address technology issues but also governance factors related to information security.

The framework outlines particular roles and responsibilities for managers in various levels i.e. the CEO, Business unit heads, senior managers and CIOs.

The other important aspect of the framework which was considered is its inclusion of a metric system for evaluating effectiveness of information security implementation.

The framework is presented in the following table.

Table 5: Proposed Information Security Governance Framework

Actors\Actions	Corporate Executives	Business Unit Head	Senior Manager	CIO/CISO
	What am I required to do? / What am I afraid not to do?			
Governance/Business Drivers	Legislation, ROI	Standards, policies, Budgets	Standards, audit results	Security policies, security operations, and resources
	How do I accomplish my objectives?			
Roles and Responsibilities	• Oversight and coordination of policies • Oversight of business unit compliance • Compliance reporting • Actions to enforce accountability	• Provide information security protection commensurate with the risk and business impact. • Provide security training • Develop the controls environment and activities • Report on effectiveness of policies, procedures and practices	• Provide security for information and systems • Periodic assessments of assets and their associated risks • Determine level of security appropriate • Implement policies and procedures to cost effectively reduce risk to acceptable levels • Periodic test of security and controls	• Develop, maintain, and ensure compliance to program • Designate security officer with primary duties and training • Develop required policies to support security program and business unit specific needs • Develop information use and categorization plan • Assist senior managers with their security responsibilities • Conduct security awareness
	How effectively do I achieve my objectives? What adjustments do I need to make?			
Metrics/Audit	Financial reporting, monetizing losses, conforming to policies	Policy violations, misuse of assets, internal control violations	Risk assessment and impact analysis, control environment activities, remedial actions, policy and procedure compliance, security and control test results	Security awareness effectiveness, incident response and impact analysis, security program effectiveness, information integrity, effects on information processing

Source: Adapted from Corner et al (2003)

CHAPTER THREE: RESEARCH METHODOLOGY

Introduction

This chapter describes the methodology applied in carrying out our research. The major areas it addresses are; the research design chosen, sources of data for the study, tools and procedure for collecting data, sampling methodology, sample size and its justification and methodology of data analysis.

3.1. Research Design

Research design was used to come up with the structure of the research in which the major parts of the research project work in harmony in addressing the central research questions Kombo and Tromp (2006).

According to Kothari (2004) research design constitutes the blueprint for collection, measurement and analysis of data.

Survey design, in which information is gathered through interviews, administration of questionnaires, use of observation and also focus group discussions to a sample of respondents Gable (1994), was used in our study. However, only questionnaires were used for collection of data.

Survey research design, which is a systematic method for gathering information through administering of questionnaires to a sample of members of the population, was used in the study. Main purpose of the design was to describe the attributes of the larger population, from the sample.

3.2. Sources of Data

In our research data was collected directly from respondents; hence primary source of data was utilized. To accomplish this, questionnaires which were administered to respondents in sampled public sector institutions in Kenya was be utilized. This source was significant for the research because questions, whose purpose was to assist gain knowledge on information security measures already in place in these institutions, were posed to the identified respondents.

3.3. Tools, Procedures and Methods for Data Collection

The research largely made use of quantitative data collection method. This method was opted for because of the following reasons.

- Data to be collected was indented to be as accurate and precise as possible. This would not have been very easy to achieve with qualitative method of data collection.
- The questions posed were largely closed-ended questions. This was indented to help in timely analysis of data and inference thereof given time limitation of the research.

In our study, self-administered questionnaires, - with largely closed-ended and short questions - were used. The questionnaires were distributed to selected persons from members of the identified sample of the population. The questions were designed such that they would not be ambiguous, they would be relevant and they would have consistency in logic. Also to enable the respondents answer the questions well, the questions were followed by short explanations where necessary.

The above data collection tool was chosen for our research because it tends to give accurate and precise data and also it is more suited especially where sampling is employed as it was the case in our study. Other reasons for settling on questionnaires as our data collection method were: -

- Cost – this method is less costly compared to other primary data collection methods
- Answers to the questions are in respondents' own words; this largely avoids bias of the interviewer.
- Respondents are usually given enough time to provide answers to the questions.
- Some respondents may not be easily approachable, but with questionnaires they can be reached conveniently for instance by mailing the questionnaire to them.

The above named benefits are noted by Kothari (2004).

3.3.1. Procedure of Data Collection

After the institutions to participate in the study were identified, then key persons in these institutions were identified mainly from the ICT sections, to participate in the study.

Questionnaire Piloting

The questionnaire used for the exercise had 5 sections as follows: -

- Section A: General Information
- Section B: Officers Responsible for various roles
- Section C: Specific Roles and Responsibilities
- Section D: Evaluation Matrix

Section E: Security Challenges Faced

Under each section, there were several questions – mainly closed ended ones – which sought to gather information relevant to the field of our study.

The first section i.e. general information sought to gather general information of the respondent e.g. their designation and number of years they had worked for the institution they were currently in.

The second section was meant to gather information about the various officers responsible for certain roles and responsibilities pertaining to information security governance in the institution.

The third section was used to gather information regarding the effectiveness of the roles undertaken by the various officers in the chain of information security governance in the institution. Fourth section - on evaluation matrix - was used to obtain information concerning the effectiveness of the matrix used for evaluating information security governance roles plaid by the various levels of officers.

Finally the fifth section's role was to gather information regarding information security breaches that have been suffered by the said institutions and the measures the respondents thought would mitigate these breaches.

After the questionnaires were received from respondents, they were examined and the data cleaned in preparation for analysis. Apart from cleaning data, it was also coded for ease of entry into the SPSS software. The data analysis, as has been hinted, SPSS version 16.0 was used to expedite the exercise.

Questions in the questionnaire were mostly closed ended and most of them used a five scale likert scale type i.e. 1=Strongly Disagree, 2=Disagree, 3=Neutral, 4=Agree and then 5=Strongly

Agree. This method type was opted for because according to Palvia et al (2001) it tends to be cognisant of the differences that exist in respondents' opinions and does not give supposition of accuracy.

Before the exercise of data collection commenced, the questionnaire was piloted to six respondents to assess its reliability. However before the questionnaire was administered to targeted respondents, steps were taken to assure the would be respondents that the information they would provide will be accorded the level of confidentiality it deserves Wei and Loong (2009)

A reliability score of 0.934 using Cronbach's Alpha analysis was obtained which is higher than the minimum acceptable score of 0.7.

Table 6: Questionnaire Reliability Analysis

Reliability Statistics	
Cronbach's Alpha	N of Items
.934	37

Source: Research

After the pre-test of the questionnaire and identification of respondents, the questionnaires developed for the purpose of data collection were administered i.e. questionnaires distributed.
The next phase, which is data analysis, has already started with some preliminary results shown in the next chapter on data analysis.

3.3.2. Sample Design

Our population of study was all public sector institutions in Kenya. The public sector has three major categories; central government, local authorities and state-corporations hence homogeneity lacking in the institutions.
Given the above layout of the public sector in Kenya, the research was to employ both probability and non-probability sampling designs.

First, because institutions either lie in one of the three categories, then stratified random sampling, where the population of study is divided in related subgroups – in our case; central, local and state corporations – was used. In either category, a simple random sample was chosen. However, especially in central government category, consideration of nature of business was to be born in choosing members of sample; this is because there were some institutions in which it was not easy to gather information from e.g. security related institutions. Therefore in this case, non-probability sampling, and more specifically purposive sampling was utilized to avoid those institutions where it was difficult to collect data from.

We intended to have a sample size which was optimal not too small hence failing to achieve the objectives of the research and not too large due to cost and likely wastage of resources. A sample of at least ten institutions from each category and at least 3 respondents from a member of the sample was thought to be an adequate sample size.

After institutions for the sample were identified, then particular respondents from each institution were identified who were to participate in the study. Nonetheless, it was planned to have the following respondents from each institution as the main respondents.

3.4. Data Analysis Methods and their Justification

Data analysis is said to be the examination of the data that has been collected in a research and making deductions and inferences; Kombo and Tromp (2006). It involves the scrutiny of collected information and making inferences.

This study intended to use confirmatory data analysis method which makes use of probability theory in the effort to answer particular questions.

This method was considered because our study was largely quantitative in nature. In quantitative data analysis, numerical values are measured and descriptions such as frequencies, mean and standard deviations are made.

Upon collecting data, statistical data analysis software i.e. SPSS version 16.0 was utilized in analysing data.

3.5. Research hypothesis

According to Kothari (2004), when one talks of a hypothesis, what usually comes into mind is just a mere assumption or supposition which can be proved or disapproved. Kothari continues to define hypothesis: -

"Hypothesis is a proposition or a set of proposition set forth as an explanation for the occurrence of some specified group of phenomena either asserted merely as a provisional conjecture to guide some investigation or accepted as highly probable in the light of established facts".

During literature review it became apparent that for an institution to have working information security implementations, there is a need for framework to guide in governance of the process. From the framework adopted, certain officers within the organization structure are tasked with specific information security governance roles which they are required to play. These roles are required to be effective; hence there is a need for them to be evaluated for effectiveness. Therefore the following hypotheses were drawn from the framework relating roles and matrices used to evaluate the roles.

H1. The effectiveness of periodic tests of security and controls has direct impact on the effectiveness of security and control test results as a matrix for evaluating information security implementations.

H2. If internal controls are effectively developed, information integrity will be an effective tool for measuring compliance to information security measures.

H3. If training on information security is carried out effectively the level of security awareness will be an effective tool for evaluation of information security measures implemented.

Hypotheses Testing

For testing of the hypotheses, linear regression analysis was utilized. The method was used because it brings out the relationship between one independent variable and other dependent variable. This will suit well in our study because we are trying to bring out the relationship that may exist between two variables.

CHAPTER FOUR: RESULTS AND DISCUSSION

4.1. Results

After data collection analysis of data was commenced. Most of the analysis was based on frequencies distribution on each variable tested. The hypotheses as shown from research methodology were tested using linear regression method.

4.1.1. Section A: General Information

On the first section, in which we mainly sought to know the number of years the respondents had worked in their organization, the following results were obtained.

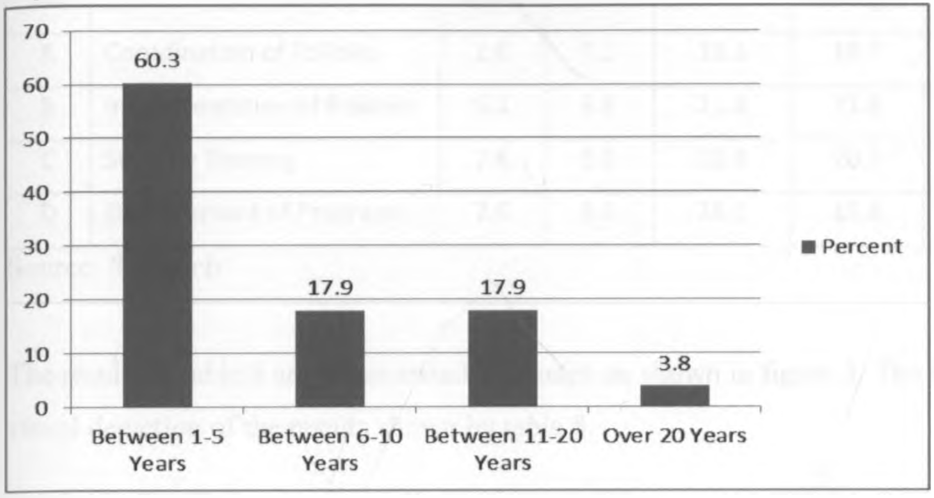
Table 7: Work Experience

Years	Frequency	Percent
Between 1-5 Years	47	60.3
Between 6-10 Years	14	17.9
Between 11-20 Years	14	17.9
Over 20 Years	3	3.8
Total	**78**	**100.0**

Source: Research

From the results, it is observed that the biggest number of respondents lie in the experience bracket of between one and five years of experience taking up 60.3%. The results can be well be depicted graphically by the following pie chart.

Figure 2: Work Experience of Participants Expressed in Percentage



Source: Research

From the figure above, it is very clear that majority of respondents lie between one and five years' of experience. This scenario may be attributed to the fact that, the public started to significantly invest in ICT infrastructure in the past few years which then called for capacity building partly by employing new young and energetic employees to man the institution's ICT sections.

4.1.2. Section B: Officers Responsible for Various Roles.

In this section we sought to know the persons responsible for certain roles in information security governance in the organization of the respondents. The roles were broadly grouped into four i.e. coordination of security policies, implementation of security policies, security training and development of program.

The results of the four groupings are shown table 8:-

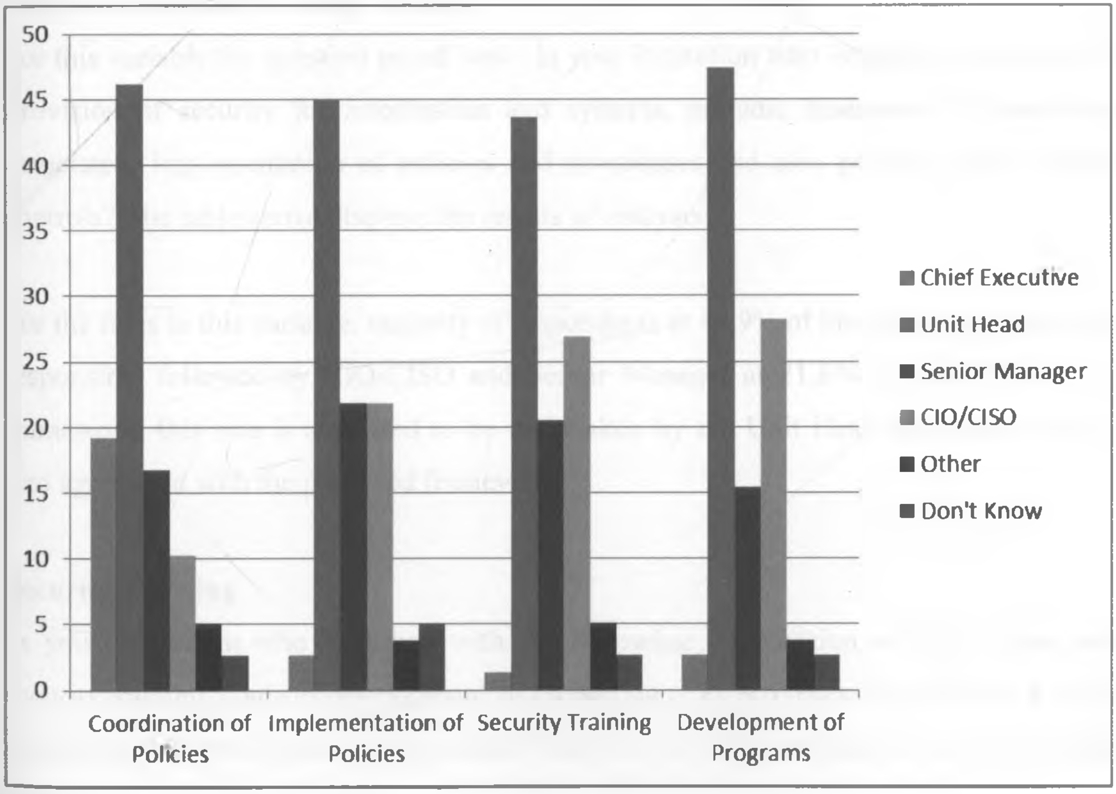
Table 8: Information Security Governance Roles

Role No.	Role Description	Don't Know	Other	CIO/CISO	Senior Manager	Unit Head	Chief Executive
A	Coordination of Policies	2.6	5.1	10.3	16.7	46.2	19.2
B	Implementation of Policies	5.1	3.8	21.8	21.8	44.9	2.6
C	Security Training	2.6	5.1	26.9	20.5	43.6	1.3
D	Development of Programs	2.6	3.8	28.2	15.4	47.4	2.6

Source: Research

The results in table 8 are summarized in a graph as shown in figure 3. The chart is used to show a visual depiction of the results shown by table 8.

Figure 3: Information Security Roles and Officers in Percentage



Source: Research

Coordination of Security Policies

For this variable the question was posed to respondents to identify who, in their institutions was tasked with the following: -
Oversight and coordination of policies e.g. information security policy, oversight of business unit compliance, compliance reporting and actions to enforce accountability

From the results on table 8, majority of respondents identified Unit Heads at 46.2% as the main officers who carry out coordination of polices and related roles. This outcome does not agree with the recommendations of the proposed framework where this role is placed in the hands of Chief Executive Officers. It is only 19.2% of respondents who identified CEO's as the officers playing this role.

Implementation of Security Policies

For this variable the question posed was:- in your institution who is tasked with the following: - Provision of security for information and systems, periodic assessment of assets and risks associated, implementation of policies and procedures and also periodic test of security and controls? The table above displays the results of analysis.

For the roles in this variable, majority of respondents at 44.9% of identified Unit Head as the one responsible followed by CIO/CISO and Senior Manager at 21.8% for each. In our proposed framework, this role is supposed to be undertaken by the Unit Head hence the results coming into agreement with the proposed framework.

Security Training

In your institution who is tasked with the following: - Provision of information protection, security training, controls development and reporting of effectiveness of policies e.g. information security policy, procedures and practices? This was the third variable in the second section and the results are as shown above.

For the above listed role, Unit Head was once more identified by the majority of participants, i.e. by 43.6% as the key person carrying the role out followed by CIO/CISO at 26.9%. This result seems not to support the proposed framework's recommendation that this role be played by a Senior Manager or person in the same level as a senior manager.

Development of Program

This was the last variable in the second section of the questionnaire. The question posed was: In your institution who is tasked with the following: - Development, maintenance of programs, development of appropriate policies to support security program, development of information categorization plans and conduct security awareness?

The results tabulated in the table above shows outcome of analysis.

The results clearly demonstrate that, majority of respondents at percentage of 47.4% of the respondents, identified unit heads to be the ones tasked with development of security programs followed by 28.2 for CIO/CISO. This goes in contrast with the recommendations of the proposed framework in which this role is supposed to be played by CIO/CISO.

4.1.3. Section C: Effectiveness of Information Security Governance.

The third section of the questionnaire set out to gauge the level of effectiveness with which the information security governance roles were played. Eighteen variables were identified for testing various aspects of information security governance.

Results of our analysis are shown in the following sections.

For the first 6 variables, the results are shown in table 9 and figure 4.

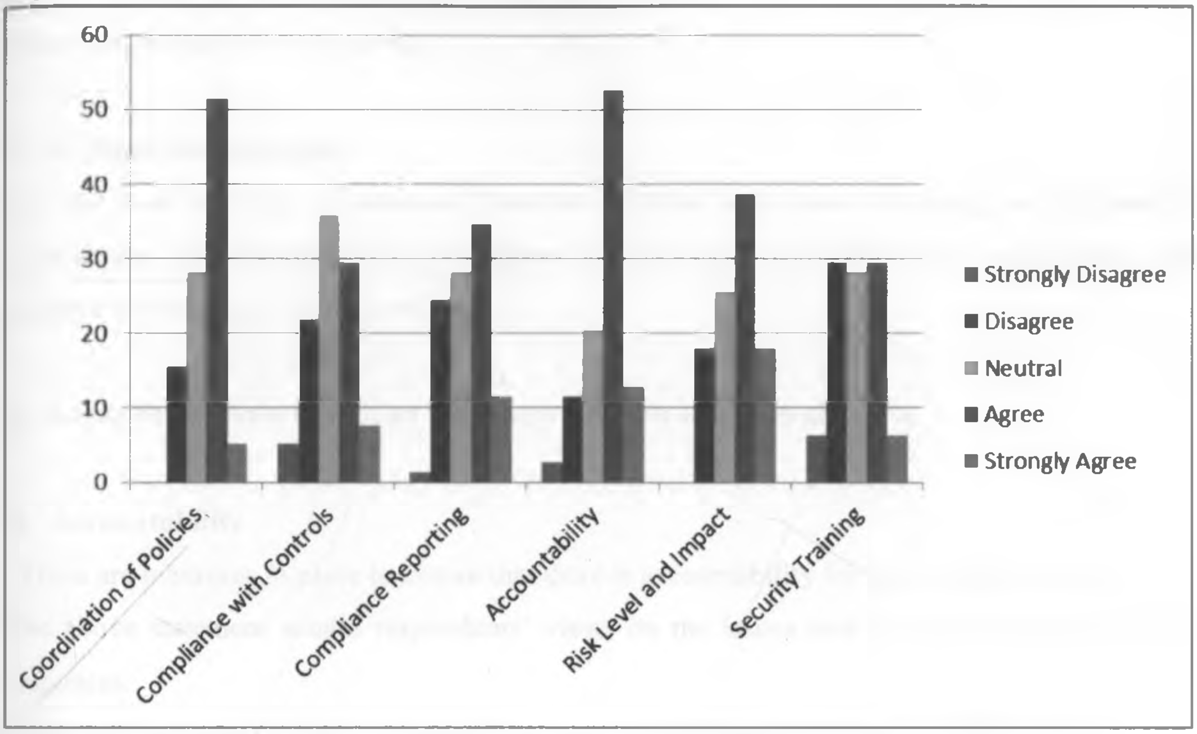
Table 9: Effectiveness of Roles (Role Number A to F)

Role No.	Role Name	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
A	Coordination of Policies		15.4	28.2	51.3	5.1
B	Compliance with Controls	5.1	21.8	35.9	29.5	7.7
C	Compliance Reporting	1.3	24.4	28.2	34.6	11.5
D	Accountability	2.6	11.5	20.5	52.6	12.8
E	Risk Level and Impact		17.9	25.6	38.5	17.9
F	Security Training	6.4	29.5	28.2	29.5	6.4

Source: Research

Figure 4 summarizes the results tabulated in table 9. The pictorial presentation of the data by the chart, affords a clear interpretation of the table.

Figure 4: Effectiveness of Roles (Role Number A to F)



Source: Research

A. Coordination of Policies

This was the first variable in the section and it sought to know the respondents' agreement with the statement that oversight and coordination of policies e.g. information security policy is carried out effectively.

The results show that the biggest proportion of respondents at 56.4% had some level of agreement with the statement. This shows that even though the players of the role may not be as per the proposed framework, the players entrusted with this role in the organization do play if with effectiveness.

B. Compliance with Controls

The second variable sought respondent's views on the statement that all departments comply with information security controls put in place.

The results on table 9 shows respondents views on the statement.

As can be seen from the results 37.2 % of respondents were in agreement with the statement i.e. either strongly agreed or just agreed. The results show that majority of participants agree with the statement, though not very strong.

C. Compliance Reporting

For the third variable, a statement "there is effective and timely reporting on the level of compliance, e.g. compliance to procedures and policies" was posed and respondents were required to view their opinions on it.

As results demonstrate there is an agreement with this statement at 46.1%.

D. Accountability

"There are measures in place to ensure that there is accountability for information security"

The above statement sought respondents' views on the issues and the table above gives their responses.

From their responses, 65.4% of respondents were in agreement with the statement whereas.

E. Risk Level and Impact

On the fifth variable in the section, respondents were required to state their level of agreement to the statement that 'information security measures are matched with the level of risk and impact e.g. high risk given high security measures."

The results of analysed opinions on the matter are given in table 9.

A majority of respondents agreed with the statement at 56.4%.

F. Security Training

"The organization has information security training programs in place" it is a statement that formed the sixth variable in the section and sought respondents' views on the effectiveness of security training programs in the organization.

Above are the results from data received on the matter.

The results show that 35.9% of respondents either strongly agreed or just agreed with the statement.

In variable number seven to twelve, the table below shows the results obtained from that exercise.

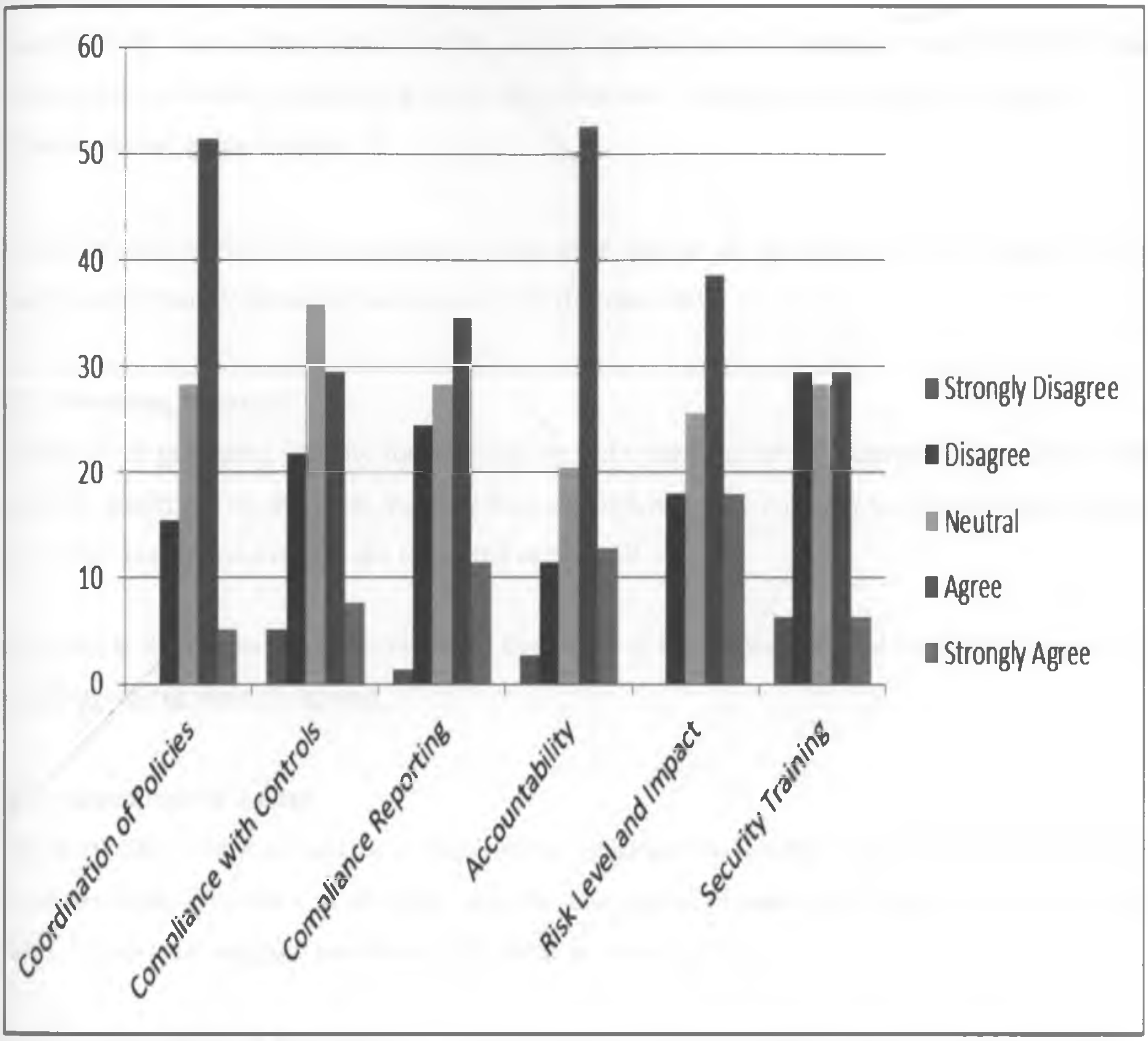
Table 10: Effectiveness of Roles (Role Number G to L)

Role No.	Role Name	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
G	Internal Controls Development		17.9	25.6	48.7	7.7
H	Reporting	1.3	19.2	32.1	38.5	9
I	Providing Security	1.3	16.7	32.1	38.5	11.5
J	Assessment of Assets	3.8	28.2	30.8	30.8	6.4
K	Level of Security		28.2	32.1	33.3	6.4
L	Implementation of Policies	2.6	20.5	33.3	41	2.6

Source: Research

Even though the numbers in table 10 depicts respondents' opinion on the questions raised, they do not afford a clear and immediate inference of the values. This possibility is clearly afforded by pictorial representation on figure 5.

Figure 5: Effectiveness of Roles (Role Number 7 to 12)



Source: Research

Internal Controls Development

In the seventh variable respondents were asked to tick their level of agreement with the statement "there are effective mechanisms in place for development of internal controls for information security".

Results are shown table 10.

56.4% of respondents agreed or strongly agreed with the statement.

G. Reporting

Respondents' views were sought in the eighth variable on the statement that "measures have been employed to ensure reporting on the effectiveness of policies, procedures and practices" The results are given in table 10.

From the results, 47.5% of respondents had some degree of agreement with the statement i.e. they either strongly agreed or just agreed with the statement.

H. Providing Security

"The role of providing security for information and systems is being undertaken effectively" this was the statement on the ninth variable that respondents were required to provide their opinion on. After analysis, the results are tabulated in table 10.

Looking at the results, it can be observed that, 50% of respondents agreed with the statement i.e. either agreed or strongly agreed.

I. Assessment of Assets

On the tenth variable on section C respondents' reaction was sought on the statement that "there is an elaborate procedure in place for periodic assessment of assets and their associated security risks." Data was analysed and results tabulated as shown table 10.

From these results, an aggregate 37.2% of respondents either agreed or strongly agreed with the statement.

J. Level of Security

"There are appropriate measures for determination of the level of security to be implemented in different areas." This was the eleventh variable that respondents were offered to state their agreement or disagreement with. After data collection and analysis, table number 10 results.

From the table, 39.7% of respondents were in agreement with the statement i.e. they either agreed or strongly agreed to the statement.

K. Implementation of Policies

Variable number twelve sought respondents' take on the statement that "implementation of policies and procedures to reduce security risks to acceptable levels is effectively done." After analysis of respondents' opinions, the results shown on table 10 were generated.

43.6% of respondents agreed with the statement whether just agreeing or strongly doing so.

The next batch of six variables are analysed in table 11.

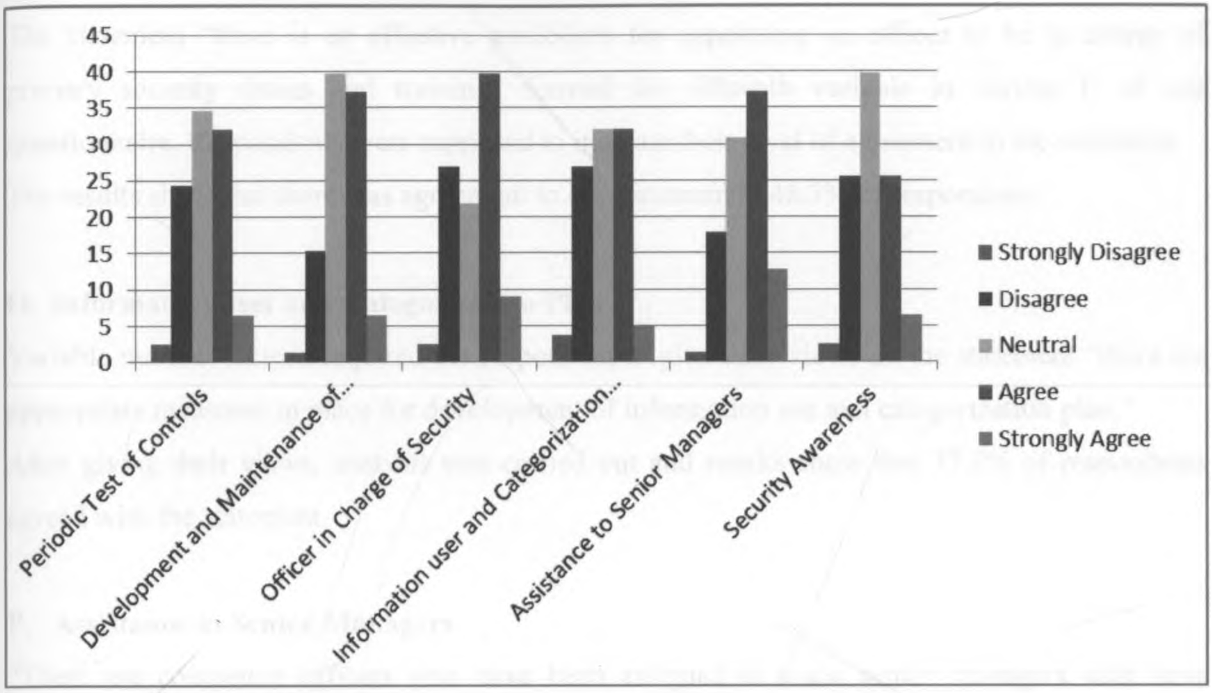
Table 11 Effectiveness of Roles (Role Number M to R)

Role No.	Role	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
M	Periodic Test of Controls	2.6	24.4	34.6	32.1	6.4
N	Development and Maintenance of Programs	1.3	15.4	39.7	37.2	6.4
O	Officer in Charge of Security	2.6	26.9	21.8	39.7	9
P	Information user and Categorization Plan	3.8	26.9	32.1	32.1	5.1
Q	Assistance to Senior Managers	1.3	17.9	30.8	37.2	12.8
R	Security Awareness	2.6	25.6	39.7	25.6	6.4

Source: Research

The results shown in table 11 are further represented in graphical format in figure 6.

Figure 6: Effectiveness of Roles (Role Number L to Q)



Source: Research

L. Periodic Test of Controls

"There is an effective mechanism in place for carrying out periodic tests on information security controls." Respondents' agreement with this statement forming variable number thirteen was sought and results are tabulated in table 11.

The results as shown in both table 11 and figure 6 show that 38.5% agreed with the statement.

M. Development and Maintenance of Programs

On the fourteenth variable, respondents were tasked to give their view on the statement; "the organization has in place effective procedures for development and maintenance of security programs." Below are the results.

From the table it is clear that 43.6% of respondents agreed with the statement.

N. Officer in Charge of Security

The statement "there is an effective procedure for appointing an officer to be in charge of primary security duties and training" formed the fifteenth variable in section C of our questionnaire. Respondents were supposed to indicate their level of agreement to the statement. The results show that there was agreement to the statement at 48.7% of respondents

O. Information user and Categorization Plan

Variable number sixteen required the respondent to give their views on the statement "there are appropriate measures in place for development of information use and categorization plan."

After giving their views, analysis was carried out and results show that 37.2% of respondents agreed with the statement.

P. Assistance to Senior Managers

"There are competent officers who have been assigned to assist senior managers with their security responsibilities." This statement making up the seventeenth variable was posed to respondents for them to agree or disagree. The results show that 50% of respondents showed some level of agreement with the statement.

Q. Security Awareness

The last variable on the section sought respondents' opinion on the statement "there are effectively followed procedures for conducting security awareness." The results show that 32% of respondents' agreed with the statement.

4.1.4. Section D: Information Security Governance Roles Evaluation Matrix

This was the fourth section in our questionnaire. The section set out to assess the effectiveness of evaluation matrix used to assess information security roles employed.

Twelve variables were utilized to fully assess the effectiveness of matrix used. Results of data analysis of this section are given in the following sections.

For the first 6 variables in this section, the results of data analysis are indicated in the following table and figure.

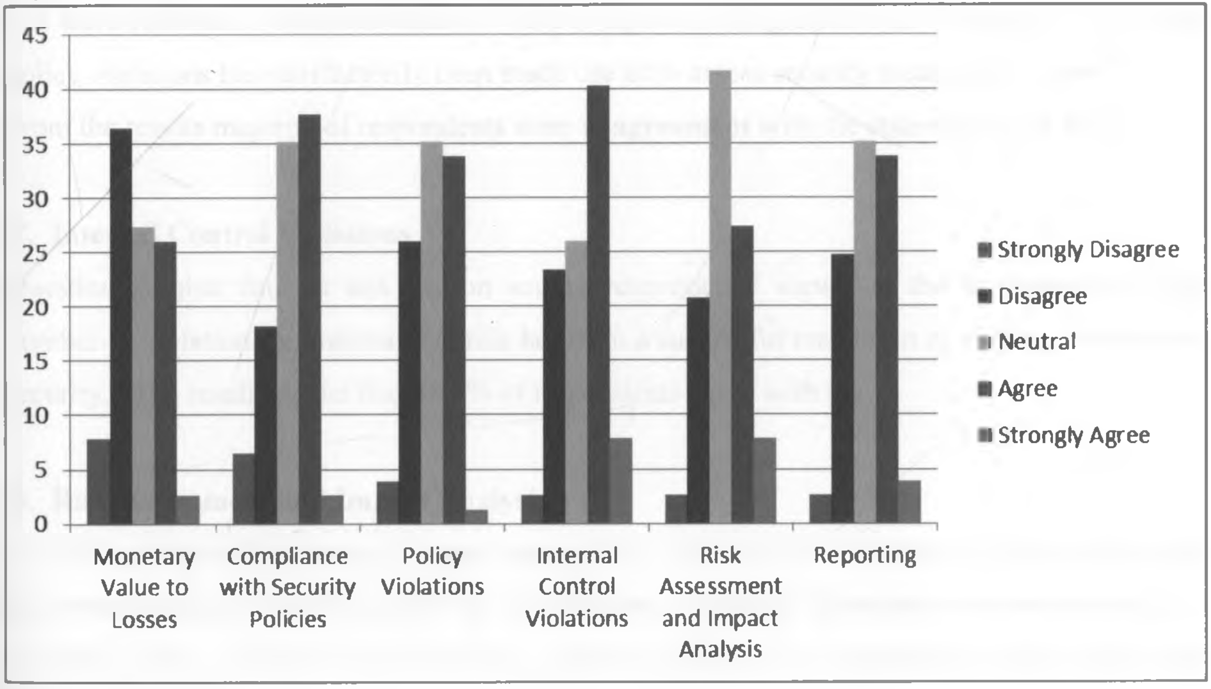
Table 12: Evaluation of Evaluation Matrix (A-F)

Role No.	Role Name	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
A	Monetary Value to Losses	7.8	36.4	27.3	26	2.6
B	Compliance with Security Policies	6.5	18.2	35.1	37.7	2.6
C	Policy Violations	3.9	26	35.1	33.8	1.3
D	Internal Control Violations	2.6	23.4	26	40.3	7.8
E	Risk Assessment and Impact Analysis	2.6	20.8	41.6	27.3	7.8
F	Reporting	2.6	24.7	35.1	33.8	3.9

Source: Research

A graphical representation of the results shown in table 12 is given in figure 7.

Figure 7 Evaluation of Evaluation Matrix (A-F)



Source: Research

Monetary Value to Losses

For this variable, the question "To what extent do you agree with the following statement regarding the level of success of information security evaluation criteria in your organization. Allocation of monetary value to losses occasioned by security risks has been employed with success." was posed and the following results were obtained.

The above results show that majority of respondents did not agree with the statement at 44.2% of those sampled.

A. Compliance with Security Policies

The second question sought respondents' views on the statement that "compliance with security policies has been a successful tool in assessing appropriateness of security measures in place." The results show that majority of respondents agreed with this statement at 40.3% of respondents.

B. Policy Violations

The third statement which respondents were to agree or disagree to was "frequency of Security policy violations has satisfactorily been made use of to assess security measures in place."
From the results majority of respondents were in **agreement** with the statement at **35.1%.**

C. Internal Control Violations

Question number four in this section sought respondents' views on the statement that "the number of violations on internal controls has been a successful method in evaluating information security." The results depict that 48.1% of respondents agree with the .

D. Risk Assessment and Impact Analysis

The fifth question purpose was to seek respondents' take on the statement that "risk assessment and impact analysis has been used with effectiveness to evaluate information systems security." Just like in the results for question four, 35.1% and 31.2% of respondents agreed and were neutral respectively.

E. Reporting

Variable number six on the section sought respondents' opinion on the statement that "reporting on the effectiveness of policies, procedures and practices has worked well in evaluating security measures." 37.7% of respondents agreed with the statement that reporting on effectiveness of policies, procedures and practices has worked well in evaluating security measures employed.

Variable number seven to twelve are listed.

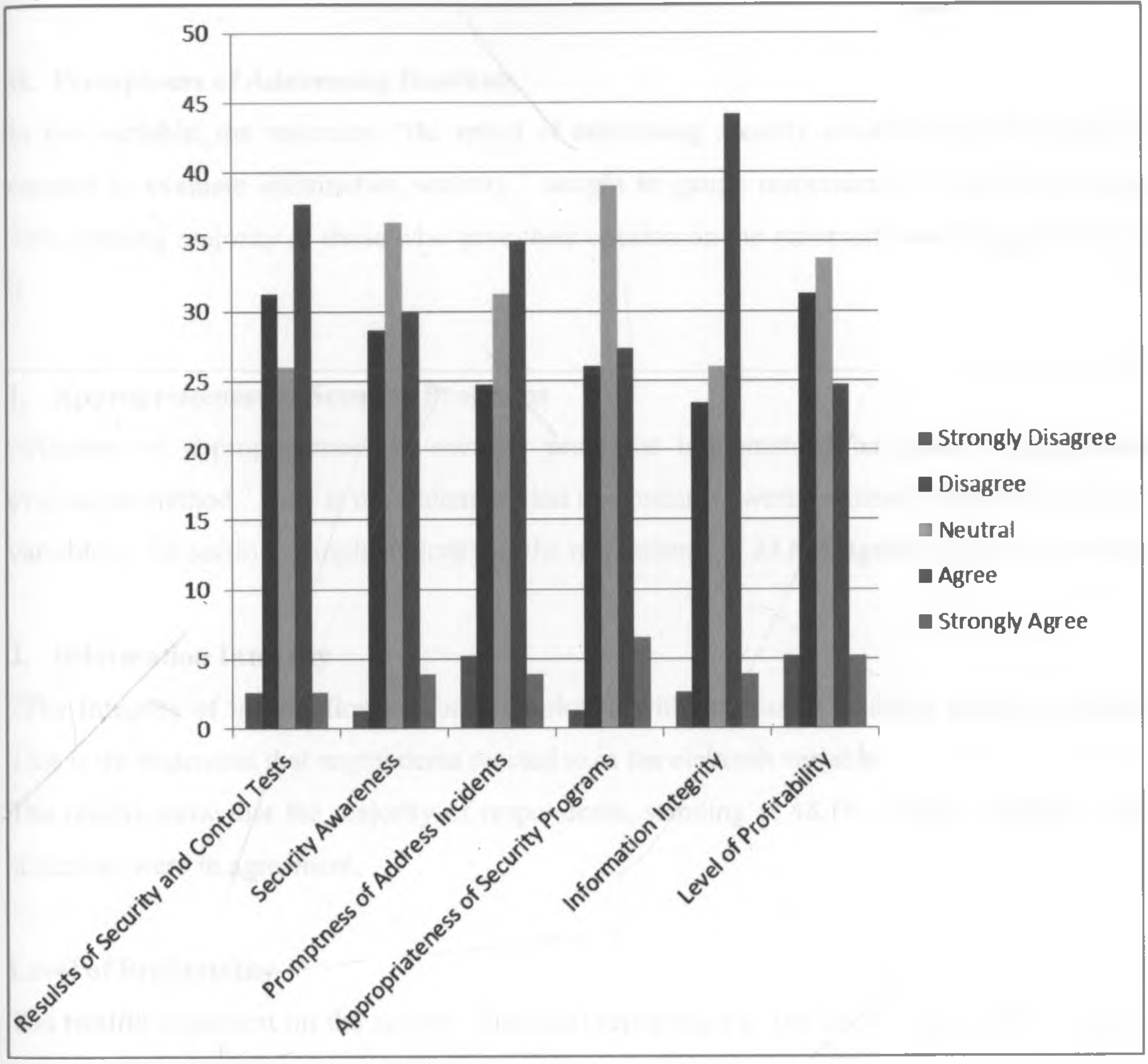
For the rest of 6 variables in this section, the results of data analysis are indicated in the following table.

Table 13: Evaluation of Evaluation Matrix (G-L)

Role No.	Role Name	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
G	Results of Security and Control Tests	2.6	31.2	26	37.7	2.6
H	Security Awareness	1.3	28.6	36.4	29.9	3.9
I	Promptness of Address Incidents	5.2	24.7	31.2	35.1	3.9
J	Appropriateness of Security Programs	1.3	26	39	27.3	6.5
K	Information Integrity	2.6	23.4	26	44.2	3.9
L	Level of Profitability	5.2	31.2	33.8	24.7	5.2

Source: Research

Figure 8: Evaluation of Evaluation Matrix (G-L)



Source: Research

F. Results of Security and Control Tests

On this variable the statement "the results of security and controls tests have been an effective security evaluation method in our organization." was posed to respondents to react to.

The results clarify that, 40.3% being majority of respondents agree with the statement.

G. Security Awareness

In this variable the opinion of respondents was sought on the statement "the level of security awareness has been used with success to evaluate security measures implemented."

33.8% forming majority of those who respondent to the statement were in agreement with it.

H. Promptness of Addressing Incidents

In this variable, the statement "the speed of addressing security incidents has been used with success to evaluate information security." sought to gauge respondents' views on the matter. 39% forming majority of those who gave their opinion on the statement were in agreement with it

I. Appropriateness of Security Programs

"Measure of appropriateness of security programs implemented has been a good security evaluation method." This is the statement that respondents' were required to react to in the tenth variable in the section. Simple majority of the respondents at **33.8% agreed** with the statement.

J. Information Integrity

"The Integrity of information has been employed with success to evaluate security measures". This is the statement that respondents reacted to in the eleventh variable.

The results show that the majority of respondents, standing at 48.1% of the respondents to the statement were in agreement.

Level of Profitability

The twelfth statement on the section "financial reporting e.g. the level of profitability has been done well in evaluating the effectiveness security policies" was to gather respondents' take on the statement. The results depict that a simple majority of 36.4% disagreed with the statement.

4.1.5. Section E: Security Challenges Faced by Organizations

This was the last section in our questionnaire. It sought to gauge the level of security challenges in form of security threats faced by organizations in the public sector in Kenya. To answer this question, three closed ended questions were posed each seeking information on different type of security threats.

To facilitate the exercise the respondents were required to tick their level of agreement with statements.

i. Malicious Software e.g. Viruses

For the first variable of the three, the question was: to what extent do you agree with the following statement regarding information security threats your organization might have faced in the past? "We have had frequent attacks from malicious software like viruses, Trojans, worms and spyware."

Results of analysis are given below.

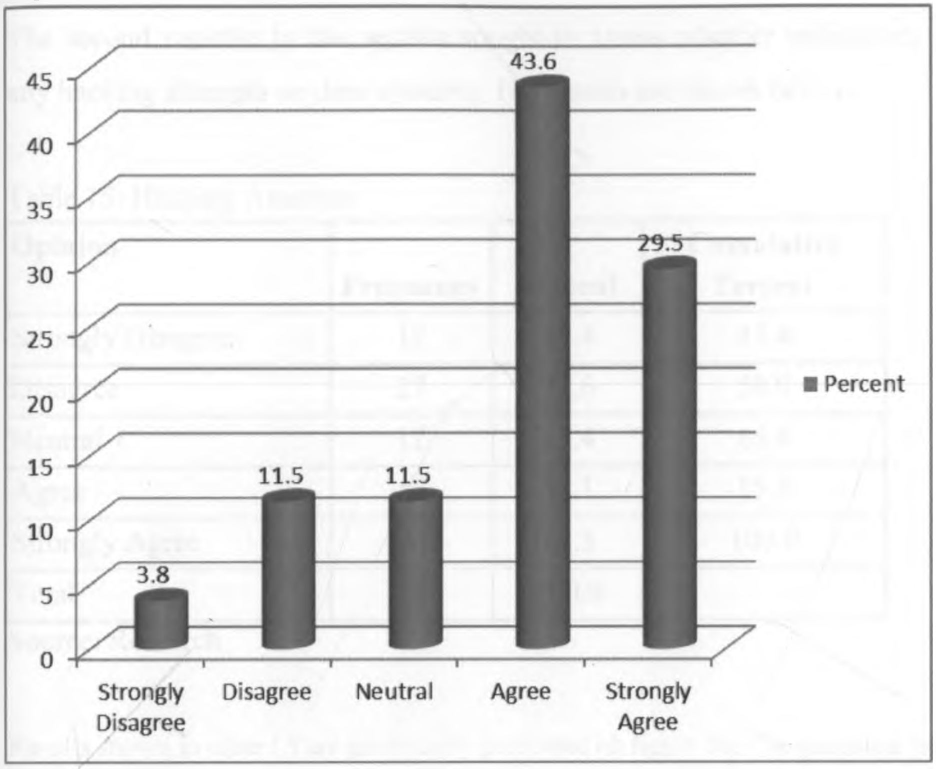
Table 14: Malicious Software e.g. Viruses

Opinion	Frequency	Percent	Cumulative Percent
Strongly Disagree	3	3.8	3.8
Disagree	9	11.5	15.4
Neutral	9	11.5	26.9
Agree	34	43.6	70.5
Strongly Agree	23	29.5	100.0
Total	78	100.0	

Source: Research

The data on table 14 is graphically represented on figure 9. This will provide a clear and easy to understand presentation of data analysis results on the security challenge of malicious software attacks.

Figure 9: Malicious Software e.g. Viruses



Source: Research

From the above results it is evident that most of institutions surveyed suffer from malicious software like viruses given that 29.5% of respondents strongly agree and other 43.6% agree that they have suffered virus attacks in the past.

ii. Hacking Attempts

The second variable in this section sought to assess whether institutions under survey suffered any hacking attempts on their systems. The results are shown below.

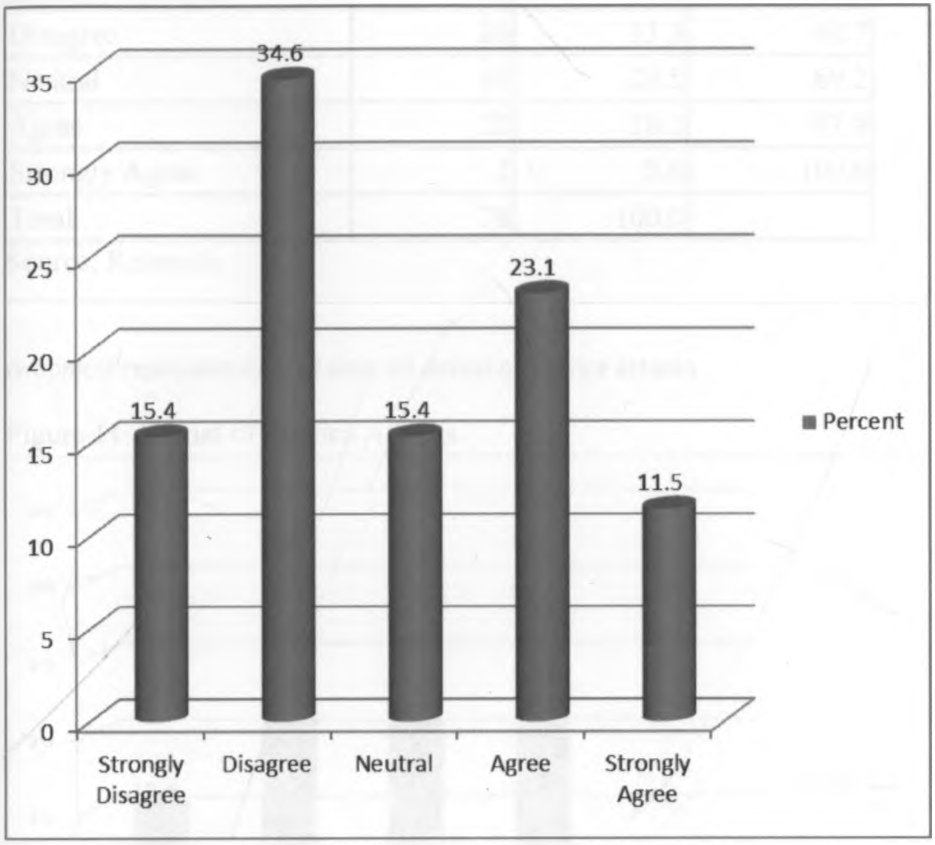
Table 15: Hacking Attempts

Opinion	Frequency	Percent	Cumulative Percent
Strongly Disagree	12	15.4	15.4
Disagree	27	34.6	50.0
Neutral	12	15.4	65.4
Agree	18	23.1	88.5
Strongly Agree	9	11.5	100.0
Total	78	100.0	

Source: Research

Results shown in table 15 are graphically presented on figure 10. The graphical presentation visually shows the outcome of data analysis on the security challenge of hacking attempts.

Figure 10: Hacking Attempts



Source: Research

From the results shown on table 15 and graphically represented on figure 10 it can be concluded that even though there are hacking attempts in the institutions, their level of 11.5% and 23.1% for those strongly agreeing and agreeing respectively are less severe compared to malware attacks which stands at 73.1 for both strongly agree and agree combined.

iii. Denial of Service Attacks

The last question on the section wanted to gauge level of denial of service attacks in institutions. The results are laid down in the table below.

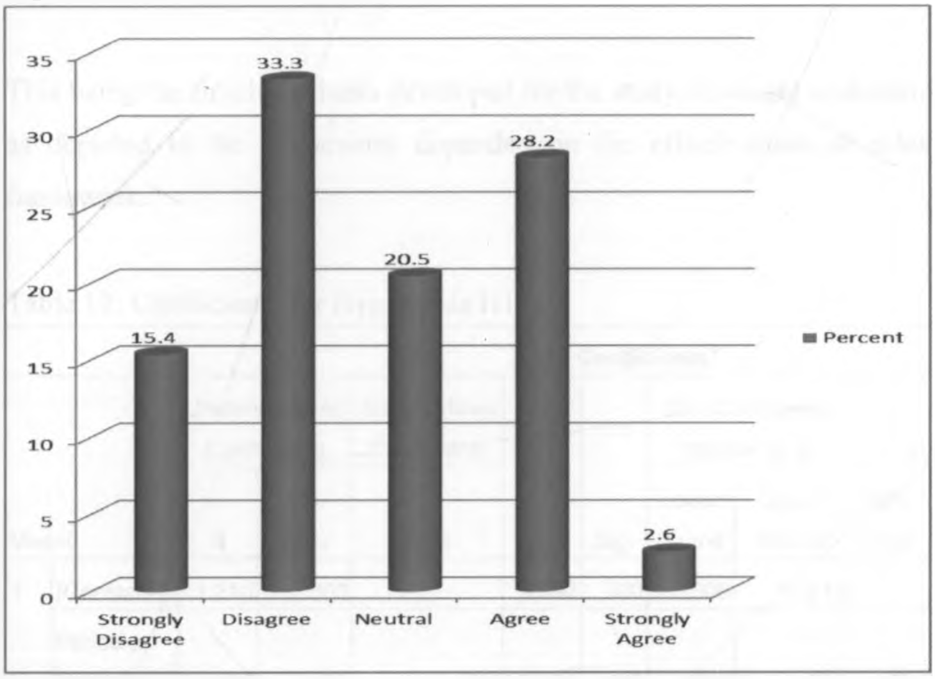
Table 16: Denial of Service Attacks

Opinion	Frequency	Percent	Cumulative Percent
Strongly Disagree	12	15.4	15.4
Disagree	26	33.3	48.7
Neutral	16	20.5	69.2
Agree	22	28.2	97.4
Strongly Agree	2	2.6	100.0
Total	78	100.0	

Source: Research

Graphical representation of data on denial of service attacks

Figure 11: Denial of Service Attacks



Source: Research

From the above results biggest proportions at 33.3% of respondents' disagree they have suffered denial of service attacks with 15.4% strongly disagreeing.

From the above analysis of security challenges faced by public institutions, most of the institutions seem to suffer from one main attack i.e. malicious software attacks. Hacking attacks and denial of service attacks seem not to have taken root in the public sector in Kenya as shown by the results.

Hypotheses Testing

Several hypotheses were developed for the research.

Simple linear regression analysis to test the hypotheses was carried out. Test results are shown below.

H1. The effectiveness of periodic tests of security and controls has direct impact on the effectiveness of security and control test results as a matrix for evaluating information security implementations.

This being the first hypothesis developed for the study, it sought to determine whether evaluation as depicted in the framework depended on the effectiveness of roles also outlined in the framework.

Table 17: Coefficients for Hypothesis H1

Coefficients^a													
		Unstandardized Coefficients		Standardized Coefficients			95% Confidence Interval for B		Correlations			Collinearity Statistics	
Model		B	Std. Error	Beta	t	Sig.	Lower Bound	Upper Bound	Zero-order	Partial	Part	Tolerance	VIF
1	(Constant)	1.210	.303		3.992	000	.606	1.814					
	Periodic Test of Controls	.588	.092	.594	6.394	.000	.405	.771	.594	.594	.594	1.000	1.000
a. Dependent Variable: Resulsts of Security and Control Tests													

Source: Research

As evidenced from the results shown in the above tables, given a significance level of 0.1%, there exists a positive relationship between effectiveness of the role of periodic tests of security and controls and control test results as a matrix for evaluating information security implementation. This is attested by the Beta value of 0.594 as shown. Therefore the hypothesis is accepted.

H2. If internal controls are effectively developed, information integrity will be an effective tool for measuring compliance to information security measures.

This hypothesis sought to determine whether there exits any relationship between information integrity as a matrix for measuring effectiveness of security and effective development of internal controls

Table 18 shows the results of analysis.

Table 18 : Coefficients for Hypothesis H2

Coefficients[a]														
		Unstandardized Coefficients		Standardized Coefficients			95% Confidence Interval for B		Correlations			Collinearity Statistics	
Model		B	Std. Error	Beta	t	Sig.	Lower Bound	Upper Bound	Zero-order	Partial	Part	Tolerance	VIF
1	(Constant)	1.374	.381		3.605	.001	.615	2.133					
	Internal Controls Development	.538	.107	.503	5.036	.000	.325	.751	.503	.503	.503	1.000	1.000
a. Dependent Variable: Information Integrity													

Source: Research

With a significance level of 0.1% the results shown in the above tables, show there exists a positive relationship between effectiveness of the role of developing internal controls and information integrity. This is confirmed by the standardized Beta value of 0.503 as shown. Therefore the hypothesis is accepted.

H3. If training on information security is carried out effectively the level of security awareness will be an effective tool for evaluation of information security measures implemented.

Table 19: Coefficients for Hypothesis H2

Coefficients[a]													
		Unstandardized Coefficients		Standardized Coefficients			95% Confidence Interval for B		Correlations			Collinearity Statistics	
Model		B	Std. Error	Beta	t	Sig	Lower Bound	Upper Bound	Zero-order	Partial	Part	Tolerance	VIF
1	(Constant)	2.114	.286		7.387	.000	1.544	2 684					
	Security Training	.318	.090	.377	3.524	.001	.138	.498	.377	.377	.377	1.000	1.000
a. Dependent Variable: Security Awareness													

Source: Research

As can be demonstrated from test results tabulated in table 19, given a significance level of 0.1%, there exists a positive relationship between effectiveness of the role of security training and effectiveness of security awareness as a matrix for evaluating information security implementation. This is attested by the standardized Beta value of 0.377 as shown. Therefore the hypothesis is accepted.

CHAPTER FIVE: CONCLUSION AND RECOMMENDATIONS

5.1. Introduction

The research set out to assess the status of information security in the public sector in Kenya. More specifically the research was to evaluate the level of information security governance within the public sector setting; this was so because in many occasions, lack of information security governance framework has been identified as one major factor affecting information security implementations Conner et al (2003). Several objectives of our research in line with the research were identified and their achievement or lack of is discussed below.

5.2. Evaluation of objectives and Questions

The study was planned in a way as to meet the objectives which were identified in the introduction section of this report. It was also expected that in the process, research questions posed will get appropriate answers. Below is the discussion on the outcomes and assessment on fulfilment of objectives.

Objective 1. The first objective of the study was to determine the effectiveness with which the public sector in Kenya was addressing the challenge of information security.

To address this objective, information was sought, by use of a questionnaire as to the effectiveness with which several roles related to information security were played in the public sector.

Responses on these questions, as demonstrated in our results and discussion chapter, shows that most of this role is played out effectively. To cite an example, 56.4% of respondents said that the role of developing information security controls was effectively carried out in their institutions. Meeting of this objective also provided an research question one which sought to

Objective 2. The second objective of our research was to identify what security challenges institutions in the public sector in Kenya faced.

To meet the objective, questionnaires were administered seeking information on whether these institutions suffered any of the three main security threats i.e. malware, hacking and denial of service.

After data analysis was carried out, it became clear that the main information security challenge faced by these institutions was attacks from malware with 73.1% of respondents having suffered from these attacks. On the contrary, most of the respondents at 50% said they had not suffered from hacking attempts a result which is close to those who had not suffered from denial of service attacks at 48.7%. Therefore, from the results, malware attacks are shown to be the main security threats whereas the other two are not as major challenges.

Objective 3. The third objective of our research was to identify the people who are responsible for information security in public institutions in Kenya.

To address this objective, questions were developed in line with the Conner et al (2003) framework. Participants were asked to identify the people in their organizations i.e. among the Chief Executive Officer, Unit Heads, Senior Managers and CIO/CISO.

From analysis of responses, it was an interesting because majority of respondents identified Unit Heads officers who are responsible for most of the roles related to information security. The results showed the following: -

i. For the role of coordination of policies, 46.2% identified Unit Heads as the responsible for the role followed by CEO at 19.2%.

ii. For the role of implementation of policies, 44.9% identified Unit Heads as responsible for the role with senior managers and CIO/CISO tying at 21.8% each.

iii. The third role was in security training. 43.6% identified unit heads as the officers responsible whereas CIO/CISO followed at 26.9%

iv. The final role for consideration was development of security programmes. 47.4% identified unit heads for the role whereas 28.2% said it was the identified CIO/CISO

Objective 4. The fourth objective of the study was to propose a framework for information security governance. The information security governance framework, having been tested through testing of hypothesis and validated is now validated and proposed for the public sector in Kenya. The framework is inclusive. It has outlined roles and respective players in information security governance who should carry out these roles. It has also come up with a matrix for evaluating the roles.

5.3. Limitations of the study.

Some aspects during research may affect the process in a negative way Mugenda and Mugenda (2003). Mugenda and Mugenda (2003) observed that limitation to be an aspect during research that may affect the outcome in a negative way. However the research has no control over limitations.

During our study we faced several limitations that are worth noting.

i. Accessibility to some of the institutions in the sample was a challenge hence affecting response to questionnaires. However this was the exception rather than the norm i.e. very few institutions posed this challenge.

ii. Our research being on security matters, respondents tended to be withdrawn at first in responding. This challenge was addressed by assuring the respondents that, the work was purely academic in nature and there will be no revelation of information provided. Secondly respondents were not required to give their names on the questionnaires.

5.4. Contributions of the Research

First and foremost, the current research expands the pool of knowledge in the field of information security. New aspects were brought out by the research especially in the public sector. For instance it was established that there existed relationship between information security roles and matrices used for evaluation of the roles.

Secondly the research validated the adopted framework on information security governance by Corner et al (2003). The validation was done using hypotheses which were tested and results are shown in Results and Discussion section of the report.

Third, to the best of our understanding, within the Kenyan public sector environment, no framework for information security governance exits. This research has validated a framework that the public sector in Kenya can use to ensure information security governance is done effectively.

5.5. Recommendations for further research

During our research, some observations were made on which further research could be carried out so as to confirm or amend the outcomes in our research.

From data analysis it became clear that, most of information security roles in public sector institutions in Kenya were being played by the Unit Heads. It is recommended for further research to be carried out to shed more light on this phenomenon.

The framework has not been tested in a real working environment of public institution in Kenya, therefore an analysis on the effectiveness of the framework when working in a real world scenario is required.

The results of the study showed that public institutions were suffering from various security threats and mostly from virus attacks. It is recommended for further research to be carried out on reasons for this situation.

This research was carried out in the public sector in Kenya. There is need for a similar research to be carried out in the private sector to determine whether the outcomes hold in the private sector environment.

REFERENCES

1. Casmir R (2005), A Dynamic and Adaptive Information Security Awareness (DAISA) Approach, Stockholm University, Department of Computer and Systems Sciences, December 2005.
2. Conner B, Noonan T, Robert W, Holleyman R.W, (2003) Information Security Governance: Toward a Framework for Action, *Business Software Alliance*
3. Fielden K. (2011), An Holistic View of Information Security: A Proposed Framework, *International Journal for Infonomics (IJI), Volume 4, Issue 1, March 2011http://www.bsa.org/country/Research%20and%20Statistics/~/media/BD05BC8FF0F04CBD9D76460B4BED0E67.ashx* – retrieved on 22 Jul 2011*http://www.iso27001security.com/html/27002.html#Section13* -retrieved on 07 Oct 2011.
4. Gable, G. (1994), Integrating case study and survey research methods: an example in information systems, *European Journal of information Systems,* **3**(2), 112-126
5. Gupta, M., & Sharman, R. (2008). Social and Human Elements of Information Security: *Emerging Trends and Countermeasures: Information Science Reference.*
6. Indiana Office of Technology, Information Security Framework: State of Indiana Information Resources Policy and Practices
7. ISO/IEC 27002:2005 Information Technology – Security Techniques – Code of Practice for Information Security Management
8. Kimwele M., Mwangi W. and Kimani S (2011), Information Technology (IT) Security Framework for Kenyan Small and Medium Enterprises (SMEs), *International Journal of Computer Science and Security (IJCSS), Volume (5) : Issue (1) : 2011*
9. Kombo D. K & Tromp D.L.A (2006), *Proposal and Thesis Writing: an Introduction*, Puline Publications Africa: Page 70.
10. Kothari C.R. (2004), Research Methodology – Methods and Techniques *New Age International (P) Ltd., Publishers,* 2nd Revised Edition.\
11. Mugenda, O. and Mugenda, A. (2003), Research Methods: Quantitative and qualitative approach, Laba-Graphics Services, Nairobi.

12. Myers, B. L., Kappelman, L. A. and Phybutok, V. R. (1997), A Comprehensive Model for Assessing the Quality and Productivity of the Information Systems Functions: Toward a Theory for Information System Success, Information Resources Management Journal, 10, 6-25

13. Palvia, S. C., Sharma R. S. and Conrath D. W. (2001), A Socio-Technical framework for quality assessment of computer information systems. Industrial Management & Data Systems, 237-251.

14. Ryan J. (2001) Information Security Practices and Experiences in Small Businesses: *Center for Information Policy Research, Harvard University, Pg 2.*

15. Sipior J. C and Ward B.T (2008), A Framework for Information Security Management Based on Guiding Standards: A United States Perspective, *Issues in Informing Science and Information Technology Volume 5, 2008*

16. Tarimo, C.N: (2006), ICT Security Readiness Checklist for Developing Countries: A Social-Technical Approach, Stockholm *University, Department of Computer and Systems Sciences, December 2006.*

17. Wei, K. S. and Loong, A. C. (2009) Measuring ERP System Success: A Respecification of the Delone and McLean IS Success Model, Symposium on progress in Information and Communication Technology, 7-12.

18. Werlinger R, Hawkey K and Beznosov K. (2009), An Integrated View of Human, Organizational, and Technological Challenges of IT Security, *Information Management and Computer Security,* Vol. 17. No. 1. (2009)

    www.in.gov/iot/files/Information_Security_Framework.pdf - retrieved on 22 Jul 2011.

APPENDICES

Appendix I: Questionnaire

Introduction:

Dear Respondent:

I am a post graduate student at The University of Nairobi studying Master of Science in Information Systems degree. I am currently conducting a research titled *"An Information Security Governance Framework in the Public Sector in Kenya"*

The main objective of this survey is to establish how public institutions in Kenya are employing information security measures. The research is purely academic, confidential and will be solely used for that purpose. The details or data provided will not be passed to any third party but will solely be used for academic purposes.

Therefore I would request you to take a few moments of your time to answer the following few questions.

Thank you very much for your cooperation.

Yours sincerely,

Nicholas M. Mbithi
MSC-IS Student
University of Nairobi

INSTRUCTIONS

- Do not write your name
- Answer all the questions
- Give only one answer per question

In sections where your response is based on five (5) point scale tick only one e.g. where;

5= Strongly agree, 4= Agree, 3=Neutral, 2= Disagree, 1= Strongly disagree.

SECTION A: GENERAL INFORMATION:

Name of Your Institution ....

How many years have you worked for the institution?

1-5 □ 6-10 □ 10-20 □ Over 20 □

SECTION B: ROLES AND RESPONSIBILITIES:

In your institution who is tasked with the following roles: - **(TICK YOUR CHOICE)**

1. Oversight and coordination of policies e.g. information security policy, oversight of business unit compliance, compliance reporting and actions to enforce accountability?

□ Chief Executive - (e.g. Permanent Secretary, Managing Director, Town Clerk)
□ Unit Head - (e.g. undersecretary, Director, Town Treasurer)
□ Senior Manager - (e.g. Financial Controller, HR Manager, Procurement Manager)
□ CIO/CISO - (e.g. Head of ICT, IT Manager, Chief Information Security Officer)
□ Other - (indicate)..
□ Don't Know

2. Provision of security for information and systems, periodic assessment of assets and risks associated, implementation of policies and procedures and also periodic test of security and controls?

□ Chief Executive - (e.g. Permanent Secretary, Managing Director, Town Clerk)
□ Unit Head - (e.g. undersecretary, Director, Town Treasurer)
□ Senior Manager - (e.g. Financial Controller, HR Manager, Procurement Manager)
□ CIO/CISO - (e.g. Head of ICT, IT Manager, Chief Information Security Officer)
□ Other - (indicate)..
□ Don't Know

3. Provision of information protection, security training, controls development and reporting of effectiveness of policies e.g. information security policy, procedures and practices?

□ Chief Executive - (e.g. Permanent Secretary, Managing Director, Town Clerk)
□ Unit Head - (e.g. undersecretary, Director, Town Treasurer)
□ Senior Manager - (e.g. Financial Controller, HR Manager, Procurement Manager)
□ CIO/CISO - (e.g. Head of ICT, IT Manager, Chief Information Security Officer)
□ Other - (indicate)..
□ Don't Know

4. Development, maintenance of programs, development of appropriate policies to support security program, development of information categorization plans and conduct security awareness?

□ Chief Executive - (e.g. Permanent Secretary, Managing Director, Town Clerk)
□ Unit Head - (e.g. undersecretary, Director, Town Treasurer)
□ Senior Manager - (e.g. Financial Controller, HR Manager, Procurement Manager)
□ CIO/CISO - (e.g. Head of ICT, IT Manager, Chief Information Security Officer)
□ Other - (indicate)..
□ Don't Know

ECTION C: ROLES AND RESPONSIBILITIES:

To what extent do you agree with the following statements regarding effectiveness of roles and responsibilities assigned to different officers? **(TICK YOUR CHOICE)**

	Strongly agree (5)	**Agree (4)**	**Neutral (3)**	**Disagree (2)**	**Strongly disagree (1)**
1. Oversight and coordination of policies e.g. information security policy is carried out effectively.					
2. All departments comply with information security controls put in place.					
3. There is effective and timely reporting on the level of compliance, e.g. compliance to procedures and policies.					
4. There are measures in place to ensure that there is accountability for information security.					
5. Information security measures are matched with the level of risk and impact e.g. high risk given high security measures.					
6. The organization has information security training programs in place.					
7. There are effective mechanisms in place for development of					

	Strongly agree (5)	Agree (4)	Neutral (3)	Disagree (2)	Strongly disagree (1)
internal controls for information security.					
8. Measures have been employed to ensure reporting on the effectiveness of policies, procedures and practices.					
9. The role of providing security for information and systems is being undertaken effectively.					
10. There is an elaborate procedure in place for periodic assessment of assets and their associated security risks.					
11. There are appropriate measures for determination of the level of security to be implemented in different areas.					
12. Implementation of policies and procedures to reduce security risks to acceptable levels is effectively done.					
13. There is an effective mechanism in place for carrying out periodic tests on information security controls					
14. The organization has in place effective procedures for development and maintenance of security programs					
15. There is an effective procedure for appointing an officer to be in charge of primary security duties and training.					
16. There are appropriate measures in place for development of information use and categorization plan					
17. There are competent officers who have been assigned to assist senior managers with their security responsibilities.					
18. There are effectively followed procedures for conducting security awareness					

SECTION D: EVALUATION MATRIX:

To what extent do you agree with the following statements regarding the level of success of information security evaluation criteria in your organization? **(TICK YOUR CHOICE)**

	Strongly agree (5)	Agree (4)	Neutral (3)	Disagree (2)	Strongly disagree (1)
1. Allocation of monetary value to losses occasioned by security risks has been employed with success.					
2. Compliance with security policies has been a successful tool in assessing appropriateness of security measures in place.					

	Strongly agree (5)	Agree (4)	Neutral (3)	Disagree (2)	Strongly disagree (1)
3. Frequency of Security policy violations has satisfactorily been made use of to assess security measures in place.					
4. The number of violations on internal controls has been a successful method in evaluating information security					
5. Risk assessment and impact analysis has been used with effectiveness to evaluate information systems security					
6. Reporting on the effectiveness of policies, procedures and practices has worked well in evaluating security measures.					
7. The results of security and controls tests have been an effective security evaluation method in our organization.					
8. The level of security awareness has been used with success to evaluate security measures implemented.					
9. The speed of addressing security incidents has been used with success to evaluate information security.					
10. Measure of appropriateness of security programs implemented has been a good security evaluation method.					
11. The Integrity of information has been employed with success to evaluate security measures.					
12. Financial reporting e.g. the level of profitability has been done well in evaluating the effectiveness security policies					

SECTION E: SECURITY CHALLENGES FACED BY YOUR ORGANIZATION:

To what extent do you agree with the following statements regarding information security threats your organization might have faced in the past? **(TICK YOUR CHOICE)**

	Strongly agree (5)	Agree (4)	Neutral (3)	Disagree (2)	Strongly disagree (1)
1. We have had frequent attacks from malicious software like viruses, Trojans, worms and spyware.					
2. We have suffered frequent hacking attempts on our systems in the past.					
3. We have experienced denial of service attacks on our network in the past.					

What are some of the ways your institution has used to address the above identified information security threats in your organization?

a) ____

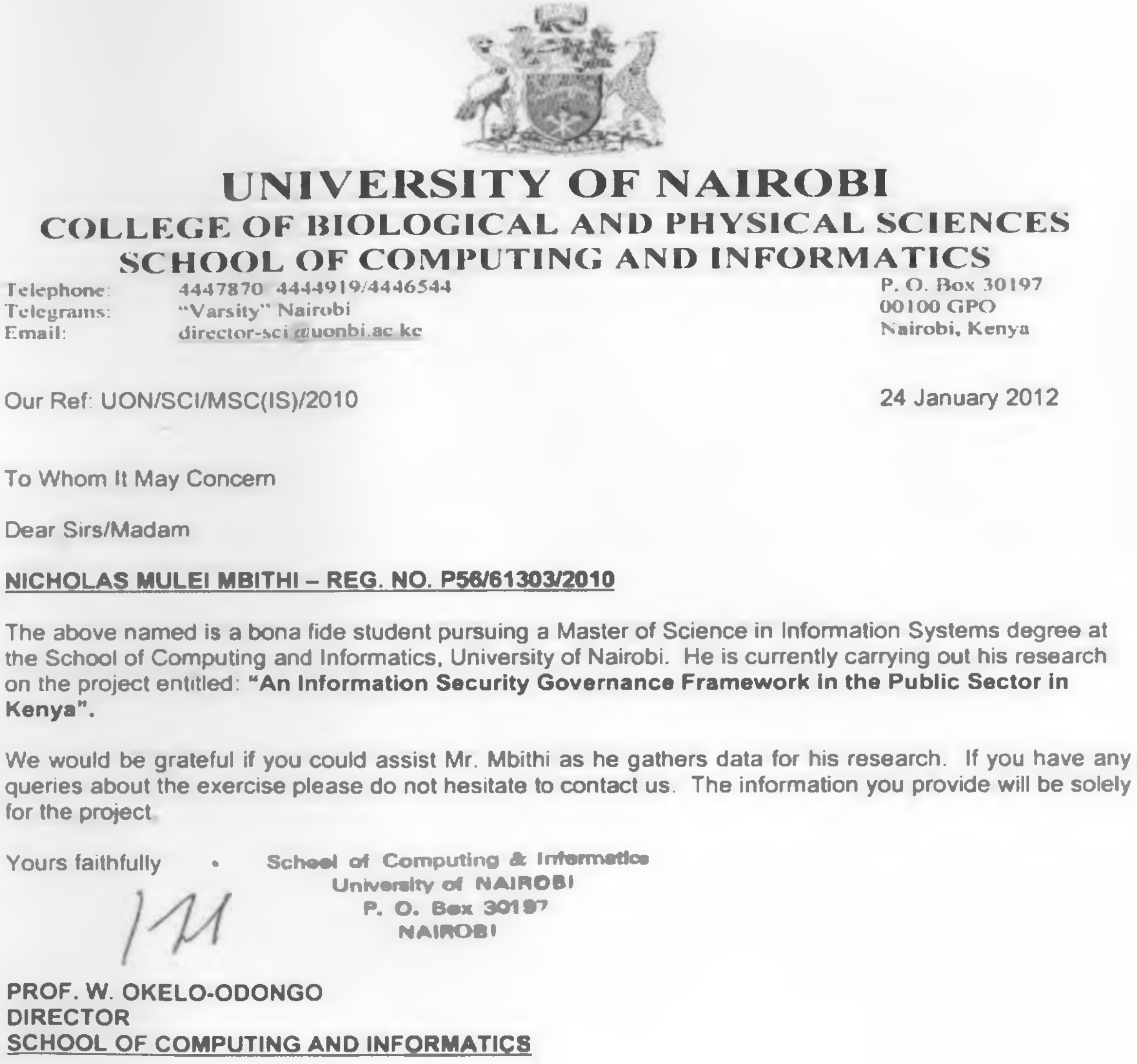
b) ____

c) ____

d) ____

THANK YOU

Appendix II: Letter of Recommendation from the University



UNIVERSITY OF NAIROBI
COLLEGE OF BIOLOGICAL AND PHYSICAL SCIENCES
SCHOOL OF COMPUTING AND INFORMATICS

Telephone: 4447870 4444919/4446544
Telegrams: "Varsity" Nairobi
Email: director-sci@uonbi.ac.ke

P. O. Box 30197
00100 GPO
Nairobi, Kenya

Our Ref: UON/SCI/MSC(IS)/2010

24 January 2012

To Whom It May Concern

Dear Sirs/Madam

NICHOLAS MULEI MBITHI – REG. NO. P56/61303/2010

The above named is a bona fide student pursuing a Master of Science in Information Systems degree at the School of Computing and Informatics, University of Nairobi. He is currently carrying out his research on the project entitled: **"An Information Security Governance Framework in the Public Sector in Kenya".**

We would be grateful if you could assist Mr. Mbithi as he gathers data for his research. If you have any queries about the exercise please do not hesitate to contact us. The information you provide will be solely for the project.

Yours faithfully

School of Computing & Informatics
University of NAIROBI
P. O. Box 30197
NAIROBI

PROF. W. OKELO-ODONGO
DIRECTOR
SCHOOL OF COMPUTING AND INFORMATICS