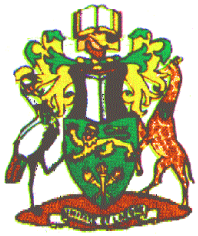


UNIVERSITY OF NAIROBI

COLLEGE OF BIOLOGICAL AND PHYSICAL SCIENCES

SCHOOL OF COMPUTING AND INFORMATICS

MASTER OF SCIENCE IN INFORMATION SYSTEMS

RESEARCH PROJECT

TITLE:

AN INFORMATION SYSTEMS SECURITY FRAMEWORK FOR KENYAN PUBLIC UNIVERSITIES

OPE JUSTUS OCHIDO

P56/72334/2008

DECLARATION

This project, as presented in this report, is my original work. It has not been presented for an award, in any other university or institution for academic credit.

Sign:_____ _____

Ope Justus Ochido Date:

P56/72334/2008

This project has been submitted as partial fulfillment of the requirements of Master of Science in information systems of the University of Nairobi with my approval as the university appointed supervisor.

Sign_____ _____

Andrew M. Kahonge Date:

University Supervisor.

DEDICATION

This Master of science research project is dedicated to my father, Mwalimu Ope Isaiah Wasonga who always reminded me to "Go back to school". My dear mother, Elsa Anyango Ope, for the love only a mother can give, My wife and children

ACKNOWLEDGEMENT

First and foremost, I wish to acknowledge the Almighty God, who not only enabled me to finish this project at His own appointed time but also gave me the knowledge to even think of starting this project in the first place.

Of great value to me, is the great support of my supervisor, Dr. Andrew Mwaura. Many thanks to you Sir, for your great support and availability to counsel, during the entire period of this project.

The panelists were great. Issues that were so complicated to me were easily pointed out and corrected with amazing ease during presentations. So I wish to appreciate each of the panelists,

I salute the dedication of the lecturers who took us through the M.Sc. course Work, I do not remember any of you missing any lecture. Many thanks to Proff. Okello Odongo and C.A Moturi for your great support with administrative issues.

To Winfred Achieng Okelo, My best friend, for your support during the course work , daughter Megan for taking me through the experience of being a student/Father.

Many people have positively influenced me in my academic journey from primary school to this level. Thank you all and may God richly bless you.

ABSTRACT

There has been rapid expansion of university education in Kenya. This has been a spontaneous response to the increasing demand for higher education necessitated by the increasing flow of students from the many secondary schools. In order to improve service delivery in these institutions, the government of Kenya has categorized its public universities as government parastatals, just like many other important, formerly, government departments. In line with this requirement, most of the public universities have adopted a computerization of their services in an unprecedented manner. Such automation often comes with new ways of exposure to frauds, which may in turn indent the corporate image of these institutions.

The purpose of this study was to establish the challenges the universities encounter in adopting and/or implementing information security policies. The study also aimed to develop an appropriate information systems security framework and assess the compliance levels for the universities in accordance to the developed frame work. The methodology used in this study involved analyzing the existing information systems security frameworks, adopting a "minimum level" security requirements for the public universities and designing a suitable information systems security framework for the universities. The methods used in the field survey included internet survey, documents review and use of questionnaire. The main finding from this study was that most universities have not developed information security frame works for their information security and reasons include lack of senior management support, lack of awareness and understanding and also technology deficiencies. Key contributions of the study include a suitable information systems security framework, identification of challenges the universities are facing in adoption and implementation of security policies. The study concludes that there is no information security policy in most public universities in Kenya and the universities need to come up with security policies which will ensure safety of their information.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER ONE

INTRODUCTION

1.1 Background of the Study

In the recent past, the government of Kenya has advertently promoted the development and use of ICT in its operations. By the year 2004, there were already 34 ministries/departments with active websites. E-government, which the government committed to making a reality by June 2004, was identified as a fundamental element in the modernization of government with a goal of making the government "more result oriented, efficient and citizen centered". Among the medium term initiatives by June 2007 was to operationalise Information Systems (IS) for key government departments and corporations like Kenya Revenue Authority (KRA), Electoral Commission of Kenya (ECK) and the National Registration Bureau (NRB) (E-government Strategy, 2004).

Currently, many more government departments/corporations not only have active websites but also have in place Enterprise Resource Planning (ERP) systems to run their core functions. The current trend in Kenya for both public and private organizations is to leverage Information Technology (IT) to provide cost effective and innovative products for the increasing number of IT literate Kenyans. E-government is taking over the delivery of services which is now done via network technologies to citizens, business and government agencies such as tax payments or license processing. One can now get services that that used to be difficult to get, like a police abstract and P3 forms from the Kenya Police website or pin certificates from the Kenya revenue authority website.

Noting that various government departments/corporations have, in the past, been mentioned adversely as being corrupt, it is possible that the corrupt practices under the manual system may be carried over to the new automated systems. Computerized systems also have new forms of threats that were not experienced under manual systems. There is therefore need for proactive and preventive measures to minimize threats to information systems security under the new (computerized) service delivery.

The Kenyan public universities are government corporations under the ministry of education. The Universities are established through institutional Acts of Parliament under the Universities Act, 2012 which provides for the development of university education, the establishment, accreditation and governance of universities. According to a 2004 report on reforming higher education in Kenya, the rapid expansion of university education in the country was a spontaneous response to the increasing demand for higher education necessitated by the increasing flow of students from schools. By the period of this research, June 2013, the number of Kenyan public universities stood at 22(check appendix for the list). An internet survey indicates that by the same period of research, all the listed public universities except Maasai Mara University have active websites from which the researcher was able to obtain a lot of information from

In 1994, the Kenya government started to implement parastatals reform project. The project, financed by the World Bank (WB) was intended to 'enhance efficiency of the public enterprises sector; reduce the financial burden of public enterprises on the public sector budget and; enable public enterprises to operate on the basis of market principles promoting operational autonomy and enhancing accountability' (WB, 2001). The state corporations are part of public sector organizations established and controlled by the government. They are created by state corporations' acts. Information systems in parastatals comprise of transaction based ISs, public sector administration and regulation information systems and public service delivery information systems just to mention but a few. The Kenya government has initiated substantial investments towards installation of ISs infrastructure in state parastatals. Funding for these investments is achieved through partnerships between the government and development partners (Magutu et al). Given the important roles played by these government corporations, there is need to have a strong policy framework on information systems security which will help in safeguarding the sensitivity of data most of which is being transformed into electronic form. .

Information security is the process of ensuring that all information created during an organization's business operations including engineering, manufacturing, marketing and other processes is appropriately protected (Schweitzer, 1990). Security risks associated with

networked enterprise system is a topic that has become increasingly significant in the recent years. Risks to a computer system can be anything from defacing a corporate website to sabotaging a metropolitan electricity distribution system and anything in between (Malioukis, 2010). Computer security addresses three important aspects of any computer-related system: confidentiality, integrity and availability.

Confidentiality ensures that computer related assets are accessed only by authorized parties. That is, only those who should have access to something will actually get that access. Access means not only reading but also viewing, printing, or simply knowing that a particular asset exists. Confidentiality is sometimes called secrecy or privacy.

Integrity means that assets can be modified only by authorized parties or only in authorized ways. In this context, modification includes writing, changing, changing status, deleting and creating.

Availability means that assets are accessible to authorized parties at appropriate times. In other words, if some person or system has legitimate access to a particular set of objects, that access should not be prevented. Availability is sometimes referred to as denial of service.

One of the challenges in building a secure system is finding the right balance among the goals, which often conflict (Pfleeger et al, 2007). Minimizing risks may require having standards and detailed security policy which would define issues such as threats and corresponding countermeasures in addition to defining rules and responsibilities. A security policy is a high level management document that informs all users of the goals of and constraints of using a system. Policy also specifies procedures, systems and tools required to protect an organization's information (Kimwele et al, 2010). A security policy must therefore answer three questions; who can access what resources and in what manner. Security policies are designed used to serve various purposes. These include; recognizing sensitive information, clarifying security responsibilities, promoting awareness for existing employees and guiding new employees. A good policy must therefore be;

Durable; It must be comprehensive/general enough to naturally apply to new cases that might arise out of unusual or unexpected ways of using a system, flexible such that an

existing policy can be applicable to new situations and changeable when it needs to be such as when government regulations mandate new security constraints.

Realistic; it must be possible to implement the stated security requirements with the existing technology.

Useful; if obscure or incomplete a security policy will not be properly implemented, if it's implemented at all. Therefore it must be written in a language that can be read, understood and followed by anyone who must implement it or affected by it.

A successful security framework relies not only upon strong leadership support but also on comprehensive body of effective and efficient information technology security policies and procedures. The policies and procedures need to: Promote public trust, Ensure continuity of services, Comply with legal requirements, Recognize risks and threats and Protect system assets**,** (Wohlever, 2009). Leadership needs to ensure that the university staff are aware of their specific information security responsibilities in the use of their information systems and the handling of those information.

1.2 Problem Statement

In order to improve on service delivery to its citizenry by the state corporations, the Kenya government policy is to leverage information technology. If well implemented, this will not only enhance efficiency of the public enterprises sector by speeding service delivery but also reduce costs regarding data protection and data security in sensitive government departments and /or corporations. As outlined in the Kenya E-government Strategy, 2004, the government has embarked on a speedy computerization of its departments. However, as evident from some reported cases in the literature review, this automation is not matched by preparedness to deal with information systems security threats. If this trend is not checked, the benefits that come with automation can instead, expose the corporations to fraud, sabotage and malicious or mischievous acts including misuse of the corporation's resources and exposure of sensitive information. Sound system security measures are mandatory if the universities as government corporations have to benefit from use of computerized services. This research investigated the level of preparedness, discovered possible causes of reported malpractices

and developed a suitable information systems security framework to help mitigate system security incidences in the institutions.

As more government Corporations begin to rely on computerized systems, so is the increase in information system security threats associated with the new technology. In this sense, there is need to investigate the level of preparedness not only in terms of technological methods but also sound policies to help counter the emerging threats and vulnerabilities. This will help in coming up with appropriate security framework for the institutions and further, help to advice the institutions' management on steps needed towards preparedness. Security risks associated with information technology, are increasing in both number and variety. Information technology network infrastructures are also increasingly becoming more complex to implement and administer. The advent of hacking tools and persons willing to distribute viruses and malicious will continue to increase the risks to IT organizations and the assets they are charged to safeguard. A greater challenge arises when dealing with a very large pool of very talented students pursuing ICT professional degree programmes (e.g., computer science, information systems, electronic engineering,). "Universities are often sources of spam or spyware and are also exposed to international hackers. Such hackers could penetrate some of the mission-critical information systems of the universities"(Rodrigues A.J, 2009)

Lack of trained I.T personnel may tempt institutions to outsource certain I.T services. Even where such arrangements are made, the outsourcing institution cannot be absolved from its responsibilities concerning information security. Each individual institution must in particular, define the value of the assets to be protected and create an awareness of information security issues with their employees, contractors, etc. This research investigated issues raised by literature and explored the practice and challenges faced by public universities in Kenya.

1.3 Research Hypothesis

Kenyan public universities do not have appropriate information systems security framework/policies to mitigate the effects of security threats to their information systems.

1.4 Research Objectives

The overriding objective of this study was to investigate the level of preparedness in dealing with information systems security threats in Kenya public universities.

The specific objectives were to:

- Develop a conceptual information systems security framework suitable for Kenya public universities.
- Asses the level of information systems security compliance if the Kenyan public universities were to adopt the suggested framework.
- Identify the challenges faced by public universities in adopting and implementing information systems security frame works.
- To investigate capability of the Kenya public universities to identify threats to their information systems..
- To establish whether universities audit their information systems

1.5 Research Questions

- What security measures are in place to detect/prevent any form of threats to the public universities' systems?
- What measurers are the Kenyan public universities taking towards adoption of information systems security frameworks/policies?
- What challenges do the universities face in adopting information systems security framework?

1.6 Research Justification

Among all the other government corporations, Kenyan public universities not only have the best educated personnel but also very intelligent young information technology students. This means that they should be at the forefront in coming up with the best information security

policies suitable even for the other Kenyan organizations. This also means that they are likely to experience information security threats from their own ever curious and intelligent university information technology students.

This study was necessary in order to unveil the correct status of the public universities in so far as security of their information systems is concerned, discover the challenges they face towards this goal and suggest possible solutions.

1.7 Significance of the study

Kenyan public universities, which have continued to grow in student population in the recent years, have adopted the use of computer-based information systems in an unprecedented manner, this automation, however, has not been matched with preparedness to counter threats usually inherent with such automation. it is important that the institutions prioritize security of their information if they have to fully benefit from the new approach to service delivery.

Research on computer crimes in Kenyan institutions show that the crimes, like alteration of university student grades, are traditional crimes simply using a computer as a tool. This research investigated the current state of the public universities on information security issues, made some recommendations and suggested a frame work to guide public universities on how to secure their systems. This research stands to benefit not only public universities implementing computer-based information systems but also other government corporations which were started primarily to rid certain government departments of corrupt practices and improve service delivery.

CHAPTER TWO

LITERATURE REVIEW

2.0 Introduction

This chapter is divided into three sections; the first section gives a review of other works done on information systems security, the second part outlines three internationally accepted information systems security frameworks and organization for economic co-operation and development (OECD) principles for IS security culture . A final part highlights some of the common security threats experienced by organizations as a result of implementation of computerized systems.

2.1 Research on Information Systems/Security

In a 2010 survey titled "U.S cost of a data breach", researchers at ponemon institute found that Data breaches continue to cost organizations more every year. The average organizational cost of a data breach in year 2010 increased to $7.2 million, up 7 percent from $6.8 million in 2009. Total breach costs had grown every year since 2006. Data breaches in 2010 cost their companies an average of $214 per compromised record, up $10 (5 percent) from 2009.

Data breaches were found to be costing more at both ends of the scale, but particularly the top. The most expensive data breach included in the 2010 study cost a company $35.3 million to resolve, up $4.8 million (15 percent) from 2009. The 2010 Annual Study: U.S. Cost of a Data Breach 6 least expensive data breach was $780,000, up $30,000 (4 percent) from 2009.

The research also found that Breach costs directly reflect IT security best practices and threat trends: the researchers noted that a consistently striking trends in the U.S. study year after year is that data breach costs more or less correlate directly with the presence or absence of major data breach causes (malicious attacks, for example) or data protection best practices (such as CISO leadership). Specifically, 2010 costs for breaches involving all major causes (malicious or criminal attacks, negligence and systems failures, as well as first timers, lost or

stolen devices and third-party mistakes) grew between 15 and 48 percent from 2009. Conversely, breaches that lacked those factors or illustrated best practices dropped even more precipitously to take the bottom rankings.

Recently reported incidences on Kenyan newspapers include one in which an Indonesian hacker attacked and defaced more than one hundred Kenya government websites in a major cyber security breach (Daily Nation, 2012), another one where a syndicate of university employees and students hacked into the institution's online database and altered examination results by impersonating former staff (Daily Nation, Friday 12, 2011), and before then, the official Kenya government police website was hacked into and defaced. According to the then police commissioner, the problem was common, only that the hackers had gone a little too far that time round (standard digital, January 6th 2011)

Kimwele et al., (2010) undertook a study on the Adaptation of Information Technology policies with focus on Kenya's Small and Medium Enterprises (SMEs). The study looked at whether the roles and responsibilities of IT security are well defined, whether they have a documented information security policy and if employees were aware of the policy. The survey concluded that much more needs to be done if SMEs are to realize the benefits of IT without compromising their security status. According to the report, 90.5% of the respondents believed that IT security is an issue SME should be concerned about, 66.7% of the respondents agreed and strongly agreed that the roles and responsibilities for IT security in their organizations are well defined, but less than 50%, that is, only 47.6% of respondents agreed and strongly agreed that they have a well documented IT security policy. Despite 47.6% acknowledging that their organizations have well documented IT security policies, only 33.3% agreed and strongly agreed that their staff are aware of the existence of such policies. This shows that there are a substantial number of SMEs with well documented policies but whose staff are not aware of the existence of such a policy.

It is also noted from the study that that only 28.6% agreed or strongly agreed that their staff are IT security educated and trained. This implies that in order to address IT security issues adequately, there's need for IT security education, from practitioners and academia. More than half (i.e. 52.4%) of SMEs surveyed agreed and strongly agreed that their staff are

informed about acceptable and unacceptable use of information systems. But from the same study, an alarming 76.2% of respondents reported that they had suffered information security breaches. These breaches included but were not limited to:

• Inadvertent breach (e.g. user accidentally deleted files or changed computer configuration)
• Deliberate attack (e.g. hacker/disgruntled staff gained access, deleting or stealing data)
• Asset theft (e.g. software application misplaced causing re-installation delay/costs)
• Equipment failure (e.g. hard drive crashed causing loss of data and business disruption)
• Back up failure (e.g. system restores failure due to corrupt/ inadequate backups)
• Data theft (e.g. espionage which resulted in data loss and possible legal exposure)
• Site disaster (e.g. fire or flood causing damage to systems and business disruption)
• Copyright infringement (e.g. staff loading pirated software, legally exposing the org.)
• Compliance (e.g. passing on confidential information, legally exposing the organization)

23.8% reported no information security breaches which may also mean that these respondents were not willing to disclose their organizations' attacks history information to outsiders. The researchers identified two main challenges which formed part of this research.

Lack of management support: Support can be termed as a major obstacle in implementing IT security policies. It's the work of SME management to ensure that the roles and responsibilities for IT security in their organizations are well defined. Only 66.7% of respondents acknowledged having their roles defined. It is usually the work of management to ensure or facilitate the development of such policies.

Lack of appropriate security training: Appropriate education and training programs help raise the awareness levels of IT security policies stated as currently at 47.6% from the research and informing SMEs about what is acceptable and unacceptable use of information systems at currently at 52.4%. Inadvertent threats pose some of the highest information security risk to SME's and yet personnel training and awareness programmes are often neglected.

In a report titled "Kenya works on training information security managers", the writer asserts that lack of training institutions for information security management has made IT

investment expensive for many organizations in Kenya, leading to some companies neglecting information security and management as integral parts of business and organizational growth. According to the report, this security challenge is the main reason government offices have resisted full computerization and digitization of all resources (Wanjiku, 2008). In a corporate setting, the computer is likely to have financial data from suppliers and credit numbers for customers, information that can be used as a tool for draining victims' bank accounts.

Improved technology, a growing number of technology savvy employees and increased access to the internet have opened the country to fraudsters. Systems that are expected to improve competitiveness have instead created loopholes for fraud (Daily Nation, 2011). In the report, a forensic and litigation services director with a reputable company asserts that there's need for proactive monitoring and logging of activity, adherence to best practice in information security, training and adequately equipping investigators.

Although some cases go unreported especially in the banking sector, there have been many cases of malpractices using electronic technology in Kenya. There should therefore be good security policies to enable Kenyan corporations in general to meet all their mission and business objectives by implementing systems with due considerations of IT related risks to the organization, its partners and customers. Such policies should cover both technical and non-technical measurers to counter threats to information systems. There should be availability of data for intended use only, integrity of system and data, confidentiality of data and system information, accountability (actions of an entity can be traced uniquely to, that entity) and assurance that the above requirements have been uniquely met (Stoneburner, 2001)

Magutu et al., (2010) in a research paper on information systems implementation in state corporations outline some challenges to implementation of IS which could also hinder the process of developing sound security measurers to counter threats to information systems. This study shows among other findings that there is lack of detailed risk management procedures which are fundamental to successful IS implementations. The study further highlights information system design and people management as one of the major challenges

to implementation of IS in the Kenyan state parastatals. The respondents revealed that, they had a problem in having their ISs up and running on time due to inefficient planning, lack of expertise, lack of mechanisms to retain qualified professional leading to poor software evaluations. About 42% of the respondents agreed that communication is not adequately done. Most parastatals, according to the study, also experience number issues and problems related to desktop computers, and installed software on compatibility issues. Problems like lack of expertise are likely to lead to incompetence in management of information systems security and thus expose the corporations to threats. In fact in their conclusions the researchers recommend the need for a research in ISs security issues in state corporations.

2.2 International Standards

In the context of this study, a security standard is a process for assisting government corporations to achieve their information systems security. It stipulates what the corporations need to do to make their information systems secure. Standards are developed in order to, among other reasons, reduce costs, create significant business value, improve business functionality, promote best practices, foster sound stewardship of public assets and assist in the protection of public assets and information. The utility of security standards goes back to the *trusted computer security evaluation criteria* that the U.S department of defense published back in1983. This commonly came to be known as the *orange book*. After a period of regional and specific country-based standardization initiatives, the international community saw some consolidation effort toward security standards. The international standards organization (ISO) has also published their own security standards, some of which overlap with other national and organization-specific criteria. Most popular of the ISO standards is ISO 17799, a standard that deals with information security management. Collectively, all standards and criteria strive for a common goal-to ensure that IS security is well understood and adequately managed (Dhillon 2007).

2.2.1 ISO 27002

The ISO 27002 standard, formerly ISO 17799, is a broad yet security-focused framework. It’s essentially a code of practice that outlines hundreds of potential controls and mechanism, which business can implement under the guidance of the ISO 27001 standard (Briggs, 2007).

The basis of the ISO 27002 standard is a document published by the UK government, which became a standard known as BS7799 in 1995. In 2000, it was published by ISO as ISO 17799. A new version appeared in 2005, along with a new publication, ISO 27001. The two documents ISO 27001 and ISO 27002 are intended to be used together with one complementing the other. ISO 27002 defines a comprehensive set of information security control objectives with best-practice security controls (Briggs, 2007). Its stated objective is to specify " the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented information security management system within the context of the organizations overall business risks". It is a framework that focuses its information security within the context of business risk. ISO 27002, therefore, reflects a very holistic and managerial approach to information technology. It addresses business continuity planning, system access control, system development and maintenance, physical and environmental security, compliance, personnel security, security organization, computer and operations management, asset classification and control, and security policy. The framework is divided into 11 modules of security as discussed below;

Security policy-the standard clearly identifies the importance of security policy. The policy provides management with direction and support for information security in accordance with business requirements.

Security organization-establishing a proper security organization is also considered central to managing security. Dual reporting structures and lack of clarity of roles and responsibilities may facilitate a security breach. The standard emphasizes the need for processes and organizational structures to be in sync.

Asset management- the standard calls for organizational assets to be identified, the argument here is that unless assets are identified, they cannot be controlled. There has to be an accounting for the assets and classification of information to indicate value and expected degree of protection.

Human resources security- this aspect is related to employee awareness about privacy and confidential issues. Organizations often establish extensive logical and computer-based controls but ignore issues like training personnel. There is need to ensure that employees, contractors and third party users understand their responsibilities.

Physical and environmental security-these aspects deal with perimeter defenses, especially protecting boundaries, equipment, and general controls such as locks to prevent unauthorized physical access to organizations premises and information.

Communications and operations management- communication controls relate to network security aspects, especially dealing with confidentiality and integrity of data as it is transmitted. Operational procedures and housekeeping involve establishing procedures to maintain integrity and availability of information processing services as well as facilities.

Access control-the aim of access control is to control and prevent unauthorized access to information. This is achieved by the successful implementation of the following objectives: control access to information; prevent unauthorized access to information systems; protect networked services; prevent unauthorized computer access; detect unauthorized activities; and ensure information security when using mobile computing and teleworking facilities.

Systems acquisition, development and maintenance-the theme of this section is that security requirements should be identified at the requirements phase of the project, the main objective here is to ensure that security is built into application systems and into overall information systems.

Information security incident management- this ensures that information security events and weaknesses are communicated in a manner allowing timely corrective action to be taken.

Business continuity management-business continuity management deals with dual objectives of counteracting interruptions to business activities and protecting critical business processes from the effects of major failures or disasters.

Compliance-this has three objectives; to avoid breaches of any criminal and civil law, statutory, regulatory, or contractual security requirements. Secondly, to ensure compliance of systems with organizational security policies and standards. Finally, to maximize the effectiveness of system audit process.

Additional factors-the standard also identifies certain factors that are critical for successful implementation of information security in organizations. These factors reflect on the importance of the organizational culture, management commitment, and risk management. The approach to implement security should be consistent with the organizational culture.

Appropriate training and education on information security should be provided to all employees.

ISO 27002 is a mature information system framework and forms the basis for the development of other security frameworks. No one security framework can address all security threats to any organization; it is therefore prudent to use a combination of reputable security frameworks in addressing the issue of information systems security in Kenya government corporations. The security framework used in the state of Ohio identifies security requirements and addresses each. The security requirements are common to many information systems and are therefore applicable to the study.

2.2.2 Ohio state information security framework

This Policy and its supporting sub policies regard the acquisition and Use of Computer and Telecommunications Products and Services and apply to all systems under the control of the Ohio Supercomputer Center (an organization which leads strategic research activities of vital interest to the State of Ohio). The framework provides understanding to the personnel responsible for developing, implementing, and reviewing information security policies and strategies in the state of Ohio. The framework is divided into seven minimum security requirements, which provide the foundation for IT security policy development. The minimum requirements as outlined in this framework may reflect the security needs of many of the government corporations. The following is a description of the framework;

Risk management; this involves risk assessment, risk mitigation and risk evaluation and assessment.

The agency risk assessments shall:

Identify IT systems, resources and information that constitute each system and prioritize the relative importance of the system assets; Identify and document potential threat-sources; Identify and document system vulnerabilities that could be exploited; Analyze security controls that have been implemented or are planned for implementation that minimize or eliminate the likelihood of a compromise occurring; Determine the likelihood of potential vulnerabilities being exercised by a threat-source; Determine the impact associated with the

compromise of agency system assets; Determine the level of risk using a rating methodology such as high–medium–low; Identify technical, operational and management controls that can mitigate or eliminate the identified risks; and Document risk assessment results and control recommendations.

Implementation of mitigation actions is based on the results of the risk assessment; Risks may be eliminated, mitigated, shared with one or more third parties, or accepted. Security controls are evaluated to determine their ongoing appropriateness and effectiveness for current and anticipated risks and update controls based upon the findings.

Confidentiality, integrity and availability; this is to ensure that internal security policies, plans and procedures address the fundamental security elements of confidentiality, integrity and availability. Businesses, citizens and employees expect that sensitive information about them will be shared only with those who need access like authorized state officials (confidentiality), that the information will not be altered either by accident or malicious intent(integrity), and that it will be available when needed(availability). There must therefore be provision of information and services only to those authorized and protection of information so that it is not altered maliciously or accidentally. Information and services must also be provided in conjunction and accordance with business continuity policy of the organization in question.

Protect Detect and Respond; this refers to the methods used to protect against, detect and respond to threats and vulnerabilities i.e measurers taken to help mitigate the risks associated with information technology resources. They are also called controls. Some controls perform more than one function related to protect, detect and respond. The table below gives an Ohio framework sample security controls and functions.

Table 2.1: Sample security controls and functions, Ohio security framework

Control	**Functions**
firewall	Protect, respond
Network intrusion detection	Protect, detect.

Automated anti-virus system	Protect, detect, respond
Identity tokens	protect
Security management system	Detect, respond
Internal security audit	Detect.

Identification and authentication, Based upon the risk assessment, Identification and Authentication process is implemented for information systems and services that require controlled access. Identification refers to the processes, policies and technologies applied to ensure that the persons, applications, servers or network devices attempting to access information resources are in fact who they claim to be. They include. a form of identification (user ID) and authentication (a password),which should be protected from unauthorized alteration and access. Passwords, PINs, biometrics, tokens and certificates are also used to ensure confidentiality, integrity and availability. Robust methods of authentication, such as two-factor authentication or digital certificates, are also employed to limit access to systems that contain data requiring more secure access or information whose disclosure would cause serious disruption or harm. This is an authentication that incorporates two elements. There are three elements of authentication: "what you know" (for example, a password or PIN), "what you have" (for example, a digital certificate or a smart card), and "what you are" (for example, a biometric).

Other important aspects of identity management include deactivation of accounts for employees that leave the corporation. Their access to corporation's information resources must be eliminated in a timely manner.

Access Control and Authorization. Access control addresses the securing of systems, both the hardware components and the software components. Authorization addresses the management of permissions to access the various system components, including processes for approving access and restricting access. Restricting access can apply to both invalid users and valid users with limited privileges. An important principle to observe is the use of least-privilege method for granting access to system assets; this is important when assigning rights and privileges to users and administrators of a system. Access control also refers to physical

security. This means the measurers to physically protect their information resource assets such as locked data rooms, locks and alarms on equipment racks, alarms and cameras at remote or back up data sites and even security guards as appropriate.

Security Audit logging. This provides a record of all activity associated with a device. The purpose of audit logging is to maintain a consistent and reliable record of system activity. When properly implemented, audit logging can serve as a preventive measure as well as a forensic aid. A comprehensive record of "who-did-what-when" can discourage asset abuse or be a vital form of evidence to prove culpability or prosecute a perpetrator. The confidentiality and security of audit information should also be ensured.

Security management and administration. This deals with the management and administration of the security policies and procedures including developing information security policy and ensuring security awareness, developing, implementing and ensuring compliance with an agency information technology security management plan, define methods for the disposal of magnetic and optical media, including the disposal of workstations containing hard drives, define methods for the disposal of sensitive information maintained electronically, define policies for changes to, deviations from, and waivers of the security management plan, understanding and explaining security requirements, defining training requirements and ensuring implementation, ensure that all security procedures are defined, documented and implemented and to establish a process for regular security self-assessments and regularly scheduled independent security assessments.

2.2.3 COBIT

COBIT is not an information security framework. In fact COBIT (Control Objectives for Information and related Technology) is an IT governance framework and supporting toolset that allows managers to bridge the gap between control requirements, technical issues and business risks. COBIT was created by the information systems Audit and Control Association (ISACA) and the IT governance institute (ITGI) in 1992. The COBIT framework process consists of 34 generic IT processes grouped into four domains: plan and organize, acquire and implement, deliver and support, monitor and evaluate. Though not an

information systems security framework, COBIT, however, identifies critical steps for information security in one of its processes. The information security includes important security objectives called COBIT security baseline and are organized into 39 essential steps to help in the planning of information security. These are outlined below; Based on impact analysis, for critical business processes, identify data that must not be misused or lost, services that need to be available and transactions that that must be trusted. The business must consider the security requirements for:

- Who may access and modify data?
- What data retention and back up are needed?
- What availability is required?
- What authorization and verification are needed for electronic transactions?

Define specific responsibilities for the management of security and ensure that they are assigned, communicated and properly understood. Be aware of the dangers of delegating too many security roles and responsibilities to one person. Provide resources required to exercise responsibilities effectively.

Consistently communicate and regularly discuss the basic rules for implementing security requirements and responding to security incidents. Establish minimum dos and don'ts, and regularly remind people of security risks and their personal responsibilities.

When hiring, verify with reference checks. Obtain the skills needed to support the enterprise security requirements through hiring and training. Verify annually whether skills are up to date. Ensure that no key security task is critically dependant on a single resource.

Identify what if anything needs to be done with respect to security obligations to comply with privacy, intellectual property rights and other legal, regulatory, contractual and insurance requirements.

Discuss with key staff what can go wrong with IT security that could significantly impact the business objectives. Consider how best to secure services data and transactions that are critical for the success of the business.

Establish staff understanding of the need for responsiveness and consider cost effective means to manage the identified security risks through security practices and insurance coverage.

Consider how automated solutions may introduce security risks. Ensure that the solution is functional and that operational security requirements are specified and are compatible with current systems. Obtain comfort regarding the trustworthiness of the solutions through references, external advice, contractual arrangements, e.t.c.

Ensure that the technology infrastructure properly supports automated security practices Consider what additional security requirements are needed to protect the technology infrastructure itself. Identify and monitor sources for keeping up to date with security patches and implement those appropriate for the enterprise infrastructure. Ensure that staff knows how to implement security in day to day procedures. Test the system, or major changes, against functional and operational security requirements in a representative environment so that the results are reliable. Consider testing how the security functions integrate with existing systems. Perform final security acceptance by evaluating all test results against business goals and security requirements involving key staff. Evaluate all changes including patches, to establish the impact on the integrity, exposure or loss of sensitive data, availability of critical services and validity of important transactions. Based on this impact, perform adequate tests prior to making changes. Record and authorize all changes, including patches(possibly emergency changes after the impact). Ensure that management establishes security requirements and regularly reviews compliance of internal service-level agreements and contracts with third party service providers. Ensure that third parties provide an adequate contact with the authority to act on security requirements and concerns. Consider the dependence on third party suppliers for security requirements and mitigate continuity, confidentiality and intellectual property risk. Identify critical business functions and information and those resources (e.g. applications, third-party services, supplies and data files) that are critical to support them. Provide for the availability of these resources in the event of a security incident to maintain continuous service. Ensure that significant incidents are identified and resolved in a timely manner.

Establish basic principles for safe safeguarding and reconstructing IT services, including alternative processing procedures, how to obtain supplies and services in an emergency, how to return to normal processing after the security incident and how to communicate with customers and suppliers. Together with key employees, define what needs to be backed up

and stored off-site to support recovery of the business (e.g. critical data files, documentation and other IT resources) and secure it appropriately. At regular intervals, ensure that the back up resources is usable and complete.

Implement rules to control access services based on the individuals need to view, add, change or delete information and transactions. Especially consider access rights of service providers, suppliers and customers. Ensure that responsibility is allocated to manage all user accounts and security tokens to control devices, tokens and media with financial value. Periodically review the actions and authority of those who manage user accounts. Ensure that these responsibilities are not assigned to the same person.

Detect and log important security violations. Ensure that they are reported immediately and acted upon in a timely manner. To ensure that counterparties can be trusted and transactions are authentic when using electronic transaction systems, ensure that the security instructions are adequate and compliant with contractual obligations. Enforce the use of virus-protection software through out the enterprises infrastructure and maintain up to date virus definitions. Use only legal software. Define policy for what information can come into and go out of the organization, and configure the network security systems (e.g. firewall), accordingly. Consider how to protect physically transportable storage devices. Monitor exceptions and follow up on significant incidents. Ensure that there's a regularly updated and complete inventory of the IT hardware and software configuration.

Regularly review whether all installed software is authorized and properly licensed. Subject data to a variety of controls to check integrity (accuracy, completeness and validity) during input, processing, storage and distribution. Control transactions to ensure that they cannot be repudiated. Distribute sensitive output only to authorized people. Define retention periods, archival requirements and storage terms for input and output documents, data and software. Ensure that they comply with user and legal requirements. While in storage, check continuing integrity and ensure that data cannot be retrieved. Physically secure the ICT facilities and assets especially those most at risk to a security threat, and if applicable, obtain expert advice. Protect computer networking and storage equipment (particularly mobile equipment) from damage, theft, accidental loss, and interception.

Have key staff periodically; Assess adequacy of security controls against defined requirements and vulnerabilities. Reassess what security exceptions need to be monitored on an ongoing basis. Evaluate how well the security mechanisms are operating. Check for weaknesses such as intrusion detection, penetration and stress testing, and test contingency plans. Ensure that exceptions are acted upon. Monitor compliance to key controls.

Obtain, where needed, competent external resources to review the information security control mechanisms. Assess compliance with laws, regulations and contractual obligations relative to information security. Leverage their knowledge and experience for internal use.

2.2.4 Culture and information systems security

As highlighted in the ISO 27002 framework discussed in part 2.2.1 above (additional factors), it's imperative to note that extensive logical and computer-based controls alone are not enough control to information systems security threats. The organizational culture too should be considered when implementing information systems security in the corporations. In 2002, organization for economic co-operation and development (OECD), identified and adopted the following 9 principles for IS security culture (Dhillon, 2007).

Awareness. Participants should be aware of the need for security of information systems and networks and what they can do to enhance security.

Responsibility. All participants are responsible for the security of information systems and networks.

Response. Participants should act in a timely and cooperative manner to prevent detect and respond to security incidents.

Ethics. Participants should respect the legitimate interests of others.

Democracy. The security of information systems and networks should be compatible with essential values of a democratic society.

Risk assessment. Participants should conduct risk assessment.

Security design and implementation. Participants should incorporate security as an essential element of information systems and networks.

Security management. Participants should adopt a comprehensive approach to security management.

Reassessment. Participants should review and reassess the security of information systems and networks and make appropriate modifications to security policies, practices, measurers and procedures.

2.3 Threats As A Result Of The New Computerized Service Provision.

With the introduction of computerized way of service provision, certain threats to information, usually associated with computerized systems arise which government corporation employees, with experience under the old non computerized systems, may not be familiar with. Some of them are discussed below;

2.3.1 Technical threats.

Spoofing; This involves guessing or otherwise obtaining the network authentication credentials of an entity (a user, an account, a process, a node, or a device). This will in turn permit an attacker to create a full communication under the entity's identity. Spoofing is whereby an attacker falsely carries on one end of a networked interchange. Examples of spoofing include masquerading, session hijacking and man in the middle attacks.

Masquerade; this is where one host pretends to be another e.g. in cases where domain names can easily be confused. A masquerade can register similar names of say a financial institution like a reputable bank and fraud unsuspecting customers.

Phishing; under this approach, an e-mail message is sent perhaps with a real logo of say, a bank with an enticement to click a link which is supposed to take the victim to the website. The unsuspecting bank customer ends up defrauded. Another version involves exploiting a flaw in a victim's web server. The victims' WebPages are overwritten or the attacker may build a false site that resembles the real one either to obtain sensitive information (names, authentification numbers, and credit numbers) or to induce the user to enter into a real transaction. "Phishing is becoming a serious problem, according to a trends report from the anti-Phishing working group. This group received over 12,000 complaints each month from March 2006, with the number peaking above 18,000 for March 2006" (Pfleeger, 2007)

Eavesdropping and wiretapping; The term eavesdrop implies overhearing without expending extra effort, just like a system's administrator, monitoring traffic through a node.

This form of attack involves just listening in. A related but more hostile term is **wiretap** which involves intercepting communications through some effort.

Session hijacking; This involves intercepting and carrying on a session begun by another entity. Suppose two entities have entered into a session; a third entity intercepts the traffic and carries on the session in the name of the other.

Man-in-the middle; Just like session hijacking; man in the middle involves an entity intruding between two others. The difference is that a man-in- the middle usually participates from the start of the session while a session hijacking occurs after a session has been established.

Threats to message confidentiality, integrity and availability

Confidentiality; networking is now very common for computerized systems**.** Due to the public nature of networks An attacker can easily violate message confidentiality (and perhaps integrity). Eavesdropping and impersonation attacks, discussed above, can lead to confidentiality and integrity failure. The following vulnerabilities, however, can affect confidentiality. These include;

Misdelivery; messages can be misdelivered due to some flaw in the network hardware. Such messages may be lost completely (an integrity or availability issue) or, in cases where a destination address is modified, may be delivered to some unintended recipient.

Exposure; between creation and delivery, a message content may be exposed in temporary buffers, e.g. switches, routers, gateways and intermediate hosts throughout the network, and in the work spaces of processes that build, format and present the message. A malicious attacker can use any of the exposures as part of a general or focused attack on message confidentiality. Passive wiretapping is one source of exposure.

Traffic analysis; if an attacker notices that there's heavy traffic; say between two senior officers of some organizations, he may be curious enough to listen.

Integrity; people are increasingly depending on electronic messages to direct and justify actions as long as the message is reasonable. This includes communication by short message service (sms) or e-mail. An attacker can take advantage of such trust to mislead by.

- Changing some or all of the content of a message.
- Replacing a message entirely, including the date, time and send/receiver identification.
- Reusing (replay) an old message.
- Combine pieces of different messages into one.
- Change the apparent source of a message.
- Redirect a message.
- Destroying or deleting a message.

These attacks can be perpetrated by in many ways including active wire tap and Trojan horse.

Availability; availability is also referred to as denial of service; attacks that affect availability are much more common in networks than other contexts. Some are accidental while others are malicious.

Transmission failure; This can be effected in various ways including, line cut, network noise making a packet unrecognizable or undeliverable, removal of a machine along transmission line or a machine can just be saturated and rejects data until it clears the overload. Most of these are temporary and automatically get fixed but a cut in single line may lead to denial of service.

Connection flooding; an attacker sends as much data to a host as the communication system can handle; the host is prevented from receiving any other data.

More sophisticated denial of service attacks use elements of internet protocols, normally used for system diagnostics. These include ping, echo, destination unreachable and source quench. **Chargen**, for example, is a process used to test networks capacity but can be used by an attacker to send series of packets which are then echoed back (echo chargen) making a host to hung in a loop. Others include ping of death (attacker sends a flood of pings to intended victim), teardrop (interferes with fragmentation of data units), syn flood (interferes with the three way connection hand shake) and smurf (attacker spoofs the source address in ping packet so that it appears to come from victim)

Traffic redirection; though quite sophisticated, a router is simply a computer with two or more network interfaces. If a router erroneously advertises to other routers that it has the best path to every address in the network, all routers will direct traffic towards it leading to the router being flooded or it will drop much of traffic. A lot of traffic will end up not reaching intended destination.

DNS attacks; a domain name server is a table that converts domain names into network addresses (domain name resolution). An attacker can redirect routing of any traffic with an obvious implication for denial of service. This can be done by overtaking a name server or causing it to cache spurious entries (DNS cache poisoning).

Other forms of threats

Noise; This is the interference of a signal due to other traffic or natural sources such s electric motors, lighting and animals. Noise, however, is scarcely a consideration in security critical applications.

Format failures; network communications work due to well-designed protocols that define how computers communicate with minimum human intervention, attackers may purposely break the rules. This may lead to software failure eventually leading to security compromise.

Malformed packets; on many occasions, the protocol handler detects a malformation and raises an error condition, however, when the error causes the protocol handler to fail, the result can be denial of service

Protocol failures; when incomplete, a protocol will not specify what action to take in a particular situation. A protocol may also have an unknown security flaw. All these kinds of errors can be exploited by attackers.

Website vulnerabilities. A website is especially vulnerable because it's exposed to the user, who can download the sites code for offline study. Using such information, to effect many attacks including;

Website defacement; quite common not only due to the visibility but also the ease with which it can be done.

Buffer overflows; also quite common on WebPages too. The attacker simply feeds a program far more data than it is expected to receive. When the buffer size is exceeded, the excess data spills over into adjoining code and data locations

Threats in active or mobile code; active code or mobile code is a general name for code that is pushed to the client for execution.

Cookies; these are not active codes but data files that can be stored and fetched by a remote server. Cookies can, however, be used to cause unexpected data transfer from client to server so they have a role to play in loss of confidentiality.

Scripts; clients can invoke services by executing scripts on servers. Since all communication is done through HTML, the server can not distinguish between commands generated from a user at a browser completing a webpage and a user handcrafting a set of orders, a malicious user can monitor this communication and use the knowledge to manipulate server actions.

Active code; A server may allow download of code to be executed by on client. The executable code is called active code. Two examples include activeXcontrols, for windows and hostile applet, a downloadable java code. The java code can cause harm to a clients system.

Auto exec by type; data files are processed by programs. In some cases the file type is implied by the file extension. An attacker can disguise a malicious active file under a non obvious file type.

Bots; from the term robots, these are malicious codes under remote control. The code objects are Trojan horses that are distributed to a large number of victims' machines. Botnets (network of bots) are used for denial of service attacks by launching attacks from many sites in parallel against victims. They are also used for spam and other bulk e-mail attacks.

2.3.2 Physical threats

These are generally threats to information security that involve human or natural disasters. These are serious security issues that should always be addressed in any security management.

Natural disasters; like any other equipment, computers are subject to natural disasters that occur to homes, stores and automobiles. They can be flooded, burned, melted, hit by falling objects and destroyed by earthquakes, storms and tornadoes. All such events can damage a computing system and may cause an organization to loose some of the processing in progress. Other disasters include building collapse, explosion and damage from falling objects. Though not natural disasters, they can also be considered in this category. These kinds of catastrophes are difficult to predict or estimate .Contingency measurers, however, have to be put in place to mitigate their effects when they occur.

Power loss; constant electricity supply is a requirement when using computers and for certain time-critical applications, loss of service from a system is intolerable. There have to be measures to deal with power failures.

Human vandals; computers and their related media are sensitive to a variety of disruptions. A vandal can destroy hardware, software and even data. Disgruntled employees, bored operators, saboteurs or people seeking excitement, are potential human attackers. Those with sophisticated knowledge of a system can use less suspicious tools e.g. car key cause harm to a computer by, for example, short circuiting a hard disk.

Unauthorized access and use; as distributed computing systems become more prevalent, protecting a system from outside access becomes more difficult and more important. Interception is a form of unauthorized access whereby the attacker intercepts data and either breaks confidentiality or prevents the data from being read or used by others (passive interception). There is also active interception whereby an attacker can opt to change or insert data before allowing it to proceed to its destination.

Theft; There are an increasing number of tiny electronic gadgets capable of storing large volumes of data. Such gadgets are very easy to carry away. Things that can be stolen include printed reports, tapes or disks which can easily be carried away. If done well, the loss may not be detected for some time. Personal computers, laptops and personal digital assistants (PDAs) are designed to be small and portable but can be misused for purposes of theft.

From the literature review, it is clear that there are a variety of threats to information that some Kenya government corporations including universities have faced and will continue to experience as a result of adopting automated methods of service delivery. The study investigated this problem and hopefully has made some contribution towards mitigating effects of such threats.

2.4 Security Requirements For The Public Universities

The question at this point would be "what are the basic information security requirements for any given university "A significant challenge for organizations is to determine the appropriate set of security controls, which if implemented and determined to be effective, would most cost-effectively mitigate risk while complying with the security requirements defined by applicable government laws, Executive Orders, directives, Policies, standards, or regulations ((NIST, 2009). NIST special publication 800-53 Revision 3, 2009 outlines Recommended Security Controls for Information Systems and Organizations. For the purpose of this study, we adopted the requirements outlined in this document as basic information systems security requirements for Kenyan public universities and went out to investigate whether such minimum requirements are met. The choice of this set of baselines is based on the fact that it considers that security risks associated with each organization do vary. It can thus be applied in several situations. Fifteen sets of requirements are identified in this publication, which are summarized below.

Access control; Like any other corporation universities need to fully control access to their information and information systems in such a way that there's only authorized access by internal users, remote access, wireless access, access from external information systems, e.t.c.. In cases where access is authorized, there may also be need for session control.

Awareness and training; The universities need to not only provide basic security training for information system users but also role based security related training to staff in order to maximize the benefits that accrue from use of information systems.

Audit and accountability; Each university needs to determine auditable events based on risk assessment and mission/business needs. They should be so efficient that the institution is well protected against an individual falsely denying having performed a particular function**(non-repudiation)**

Security assessment and authorization; the universities need to monitor information systems connections on an ongoing basis, and verify enforcement of security requirements. This may involve employment of independent assessment of security controls in the information systems.

Contingency planning; public universities continue to reference their former students to potential employers of former students. corporations need to put in place comprehensive contingency plans for their information systems which should be in line with other plans such as business continuity, continuity of operations, crisis communications, critical infrastructure, cyber incident response and occupant emergency plans.

Identification and authentication; the universities information systems need to uniquely identify and authenticate its users or processes acting on their behalf. This should include obscuring feedback of authentication information to avoid misuse by unauthorized individuals.

Incident response; noting that security incidents may occur, universities need to implement incident handling capability for security incidents which includes preparation, detection and analysis, containment, eradication and recovery.

Maintenance; while they need to schedule repair/maintenance of system components in accordance with the university or vendor specifications, these activities- local or non-local maintenance activities, must be authorized, monitored and controlled.

Media protection; universities need to not only restrict access to certain types of digital and non-digital media but also sanitize them prior to disposal or release for re use.

Physical and environmental protection; the universities need to restrict access to facilities where information systems reside. Restriction should also include information distribution and transmission lines within the organizational facilities. Such protection is not only restricted to physical access but also damage from power equipment, temperature control, e, t, c.

Personnel security; many information security incidences involve people. The universities need to ensure that new personnel with specific roles on the information systems are screened and their logical or physical access reviewed during transfer or termination. Such screening should include third party personnel e.g. service providers.

Risk assessment; universities need to perform security categorization which describes the potential adverse impacts to the organizational operations, organizational assets and individuals should the information and information systems be compromised through loss of confidentiality, integrity or availability.

Systems and services acquisition; universities need to consider system security during acquisition. External I.S providers must be screened to comply with organizational IS requirements and employ appropriate security controls including secure shipping of components.

System and communications protection; The universities must not only prevent unauthorized and unintended information transfer but also restrict the ability of users to launch denial of service attacks against other information systems and networks. There's also need to ensure data confidentiality while on transmission.

System and information integrity; universities need to ensure that information flowing within their system and networks are in fact true and /or trustworthy.

2.5 Evaluation of the internationally recognized security frameworks

After observations from the literature review, it is necessary to asses each of the three standards discussed in section 2.2. We need to establish the ability of each of the frameworks in addressing the requirements for the Kenya government corporations as identified in section 2.3. We look at each of the requirements visa-v each module of the existing frameworks. This method was chosen because it can best unearth the possibility of one framework not addressing all the identified requirements. It also revealed that a security requirement may be addressed in parts by more than one module. The following table summarizes These Observations.

Table 2.2: **Analysis of Reputable I.S Security Frameworks**

Corporations' Security Requirements	**ISO 27002**	**CoBiT**	**Ohio State.**
Access control	Very well addressed under access control module.	Quite well addressed in modules 30, 36 and 37.	Very well addressed under access control and authorization module.
Awareness and training	Mentioned under additional factors and human resources security. Moderately addressed.	Quite well addressed in module 5.	Mentioned under management and administration baseline.
Audit and accountability	Not addressed	Moderately addressed under module 27	Very well addressed under the security audit logging module
Security assessment and authorization.	Not addressed	Addressed in module 15 and 39, assessment and module 30 Authorization.	Not addressed.
Contingency planning.	Well addressed in its business continuity and information security incident management modules.	Quite well addressed in modules 23, and 24.	Not addressed.
Identification and authentication.	Not addressed.	Well addressed in step 1.	Very well addressed in the identification and authentication module.
Incident response	Addressed under information security incident management module.	Addressed in module 3	Not addressed
Maintenance	Maintenance security, not addressed	Not explicitly addressed	Not explicitly addressed
Media protection	Not addressed	Addresses security of back up in module 35 &37.	Well addressed under security management and administration
Physical and environmental protection	Very well covered under physical and environmental security.	Addressed in section 36	Addressed under access control and authorization
Personnel security	concerned with awareness of staff security responsibilities	Very well covered in parts 2,3,4,5 and 6	Addresses awareness of personnel to security responsibilities

Risk assessment	Not well addressed, mentioned under additional factors.	Addressed in modules 7 to10	Quite well addressed under the risk management part.
System and services acquisition	Moderately addressed under system acquisition dev.& maintenance	Not addressed	Not addressed.
Systems and communications protection	Addressed under communications and operations management	Moderately covered in module 34	Covered under confidentiality integrity and availability
System and information integrity	Briefly addressed under communications& operations management	Addressed in part 33 and 35	Addressed under confidentiality, integrity and availability

2.6 Justifications for a security framework appropriate for Kenyan public universities

While some of the identified requirements like, access control and physical and environmental protection are thoroughly addressed by the existing information security frameworks, we observed that some very important requirements are not fully addressed.

Corruption, which is one of the key reasons why the Kenya government initiated corporations, is perpetuated by personnel charged with various responsibilities within the corporations. We therefore realize the need for a framework that thoroughly addresses the issues like personnel security, awareness and training and organizational culture. Such a framework would ensure that issues such as non-repudiation are very well taken care of. Two of the frameworks address personnel training in so far as making them aware of their IS security responsibilities are concerned. Not much of organizational culture, however, is addressed.

Only CoBiT security baseline addresses the issue of personnel security thoroughly including the need to verify with reference checks during recruitment of new staff, hiring the right staff and training them.

Based on the evaluation carried out above, it became necessary to develop an information systems security framework that would more comprehensively address the identified security requirements for the Kenyan public universities in line with Kenyan organizational culture.

CHAPTER THREE:

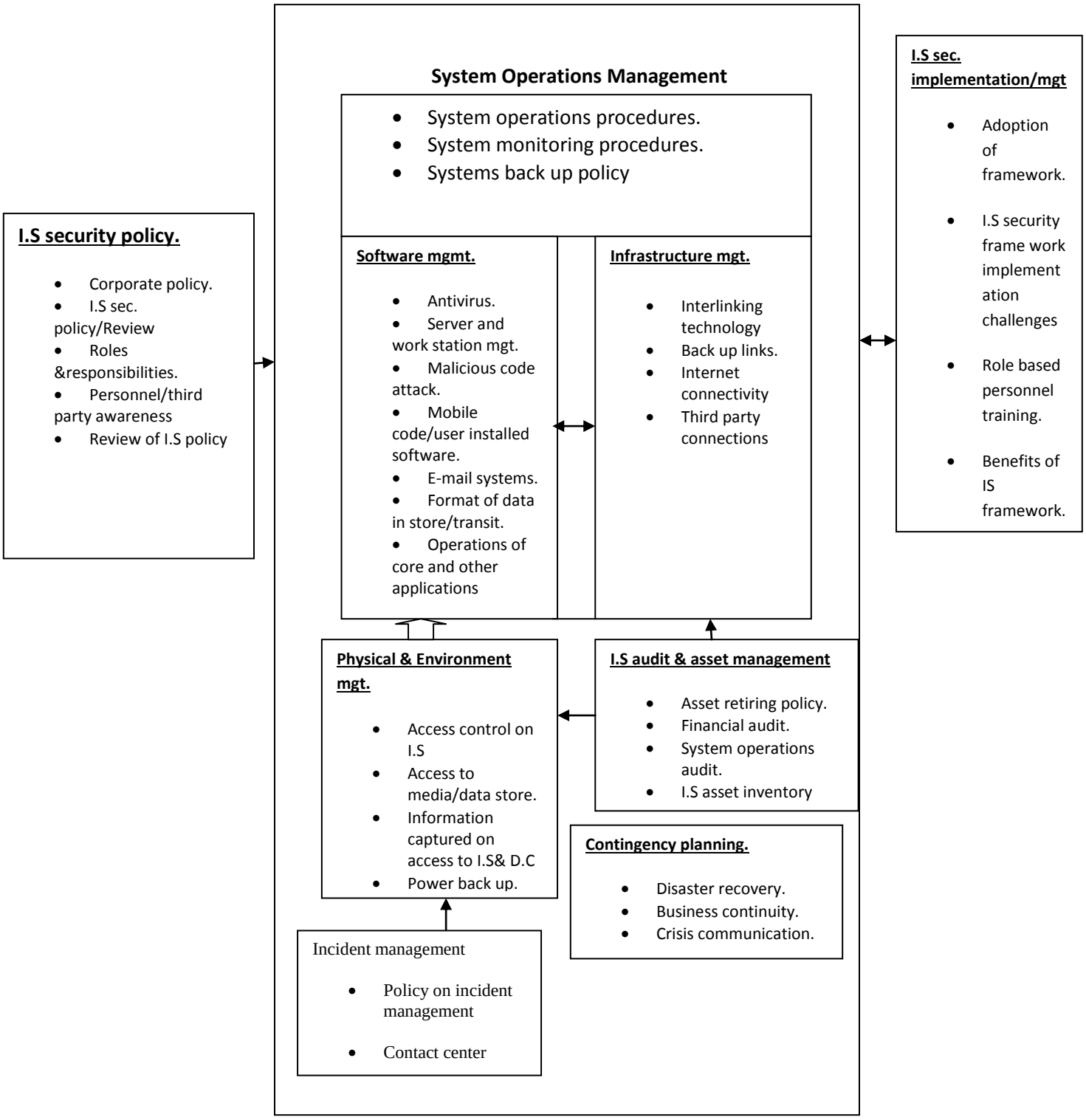
THE CONCEPTUAL FRAMEWORK

3.1Introduction

This chapter introduces a conceptual frame work. The conceptual frame work is mainly developed based on contributions from the three internationally recognized frame works; the ISO 27002, Ohio state information security frame work and CoBiT detailed within the literature review. It is then divided into seven broad subdivisions to comprehensively cover the research objectives which include; To identify the challenges faced by public universities in adopting and implementing information systems security frame works, To investigate capability of the Kenya public universities to identify threats to their information systems, To establish whether universities audit their information systems.

The following diagram represents a conceptual I.S security frame work derived from literature review. Various modules from each of the international frame works contributing to the development of this framework are highlighted below the diagram.

Figure 3.1: Conceptual Information Systems Security Framework



The **systems operations management** module of the framework deals with the general management of the system operations. It concerns administration and maintenance of operating stability and efficiency. It ensures the security of network systems and infrastructure including purchase, deployment and configuration of both software and hardware. It manages both the network infrastructure and software. This is where measurers are implemented to monitor and identify threats to organizational information systems.

Software management concerns security measurers related to software including use of appropriate/valid antivirus software, malicious code attack and e-mail systems. E-mail management can be broken down into a number of components: mail flow, storage, and user access – both at the server and user levels. Most of the public universities now have e-mail systems which can be used for various purposes including submission of student marks. Proving who has sent or received email is already a lawful requirement for many industries. This is because email can often be used as evidence in fraud and human resource court cases.

Infrastructure management ensures security of data /information on transit. These two modules work hand in hand to facilitate information security during system operations. This module is contributed to by COBIT (PARTS 10, 11,24,29,35 and 37) and Ohio State I.S frame work (part C)

Information security policy; Policies are formulated which lays down corporate response to situations and circumstances that may arise. The policy should clearly state personnel roles and responsibilities; personnel and third party awareness of the policy should be ensured. Such a policy should be such that it provides direction and support for information security. This module is contributed to by ISO 27002(part b and part d), and CoBiT (2, 3, and 5)

I.S Security implementation and management; this module deals with implementation and management of information systems security policy. At operations level, I.S personnel have the responsibility to implement an adopted or developed I.S security framework. Depending on the adopted frame work, staff training at this level is based on respective roles. An elaborate I.S framework covers both software and infrastructure management. This module is contributed to by ISO 27002(a) and COBIT (2)

The fourth module, **physical and environmental protection** deals with perimeter defenses generally preventing unauthorized physical access to organization's premises and information. It handles not only the control of physical access to the facility where information system resides but also information system distribution and transmission lines and information system input/output devices to prevent access by unauthorized individuals. An attack on physical and environment security may lead to unauthorized access and damage to system software and infrastructure.

This module therefore, handles protection to both **software and infrastructure** modules discussed above. An incident on the physical and environmental module would definitely affect both modules. An incident management module concerns how the corporation implements incident handling capability for security incidents.

Incident management involves containment, eradication, and recovery from an incident, among other responsibilities. It is prudent to have a contingency planning module to deal with incidences whose end results may be adverse effects on the physical and environmental modules.

The seventh module, **I.S audit and asset management**, is an independent module which has a dual purpose; general management of I.S assets both in use and on retirement, and systems audit, including financial audit as a consequence to information system threats.

3.2 Observations

There are generally very little information and/or research outcomes available concerning information systems security in Kenya for both private and public corporations including the public universities.

There is also no specific information security framework for the Kenya public universities

There was therefore a need to carry out research on the information systems security in Kenyan public universities.

CHAPTER FOUR

RESEARCH METHODOLOGY

4.1 Introduction

This chapter describes the research methodology that was used by indicating the research design, target population, data collection method, and data analysis that was utilized to investigate the level of preparedness in dealing with information systems security threats in Kenyan public universities.

4.2 Research Design

In order to investigate the level of preparedness in dealing with information systems security threats in Kenya public universities, the researcher adopts a descriptive research design. A descriptive research design is an in-depth investigation of an individual or a group or an institution with a primary motive to determine factors and relationships that have resulted in the behaviour of the study (Robson, 2002). The researcher undertook his research on public universities. The research design enables the researcher to undertake an in-depth investigation on the level of preparedness in dealing with information systems security threats in Kenya public universities.

4.3 Target Population

The target population for this study comprises of all senior employees in IT department in four Public Universities. The target population consists of 86 senior employees from the IT departments in Public Universities in Kenya.

4.4 Sampling Procedure

To overcome the limitations of this study the researcher employed purposive sampling and simple random sampling to select twenty six (26) respondents from the target population. Purposive sampling was used to select respondent from University of Nairobi, Kenyatta University, Jomo Kenyatta University of Agriculture and Technology and Moi University. Simple random sampling was then used to proportionately select respondents from each

University at 30.2% representative of the study's population. According to Mugenda and Mugenda (2003) a good sample population should be 10% to 30% of the entire population, this study selected 30.2%% of the entire population, which is above the recommended threshold of 30%.

4.5 Data Collection

This study collected both primary and secondary data relating to the level of preparedness in dealing with information systems security threats in Kenya public universities. Primary data was collected by use of questionnaires. The questionnaires contained open and closed ended questions and was divided into two sections, A and B. Section A focused on the profile of the respondents while section B contained questions on the research objectives. The questionnaires were administered through drop and pick from the respondents after a reasonable period of time. Secondary data was gathered from organization reports, publications and other literature relating to the level of preparedness in dealing with information systems security threats in Kenyan public universities.

4.6 Reliability and Validity of the Instrument

4.6.1 Pilot Test Report

A pilot study was carried out with 10 employees, who were not included in the actual survey. The pilot enabled the researcher to be familiar with research and its administration procedure as well as identifying items that required modification. The results helped the researcher to correct inconsistencies arising from the instruments, which ensured that they measured what was intended. Reliability refers to the consistency of measurement and is frequently assessed using the test–retest reliability method. Reliability is increased by including many similar items on a measure, by testing a diverse sample of individuals and by using uniform testing procedures. Reliability of the research instrument was enhanced through a pilot study that was done with 10 employees. The pilot data was not included in the actual study. The pilot study allowed for pre-testing of the research instrument. The clarity of the instrument items to the respondents was established so as to enhance the instrument's reliability.

4.6.2 Reliability Analysis

Reliability of the questionnaires was evaluated through Cronbach's Alpha which measures their internal consistency. The Alpha measures internal consistency by establishing if a certain item measures the same construct. Nunnally (1978) established the Alpha value threshold at 0.6 which the study benchmarked against. Cronbach Alpha was established for every objective in order to determine if each scale (objective) would produce consistent results should the research be done later on.

4.7 Data Analysis and Report Writing

Before processing the responses, the completed questionnaires were edited for completeness and consistency. A content analysis and descriptive analysis was employed. The content analysis was used to analyze the respondents' views about the level of preparedness in dealing with information systems security threats in Kenya public universities. The data was coded to enable the responses to be grouped into various categories. Descriptive statistics such as means, median, mode and standard deviation were used to help in data analysis. Tables and other graphical presentations, as appropriate, were used to present the data collected for ease of understanding and analysis. Factor analysis was applied to determine the relative importance of each of the variables with respect the level of preparedness in dealing with information systems security threats in Kenya public universities.

CHAPTER FIVE:

RESULTS

5.1 Introduction

This chapter presents analysis and findings of the research. From the study population target of 26 respondents, 21 respondents filled and returned their questionnaires, constituting 81% response rate. Data analysis was done through Statistical Package for Social Scientists (SPSS). Descriptive statistics was used to analyze the data. In the descriptive statistics, relative frequencies were used in some questions and other were analyzed using mean scores with the help of Likert scale ratings in the analysis.

5.2 Demographic Information

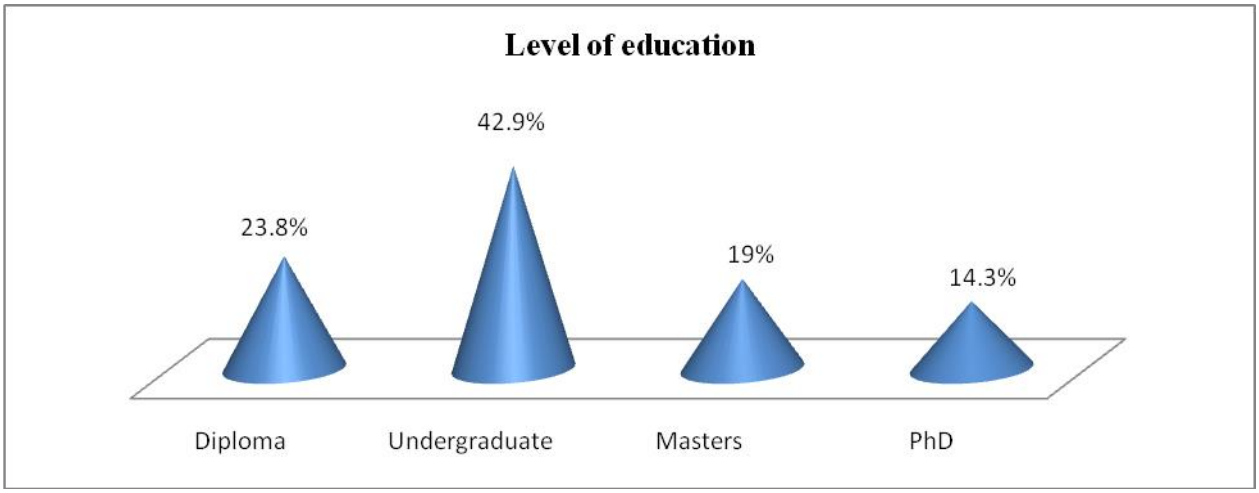


Figure 5.2: Level of Education

From the findings on the respondents highest level of education, the study found that 42.9% of the respondents indicated that they were in possession of bachelor's degree , 23.8% of the respondents had attained diploma level of education , 19% of the respondents indicated that they had attained masters level of education whereas 14.3% of the respondents were in possession of PhD. This was an indication that majority of the respondents were well educated and were in a position to understand and give credible information to the study.

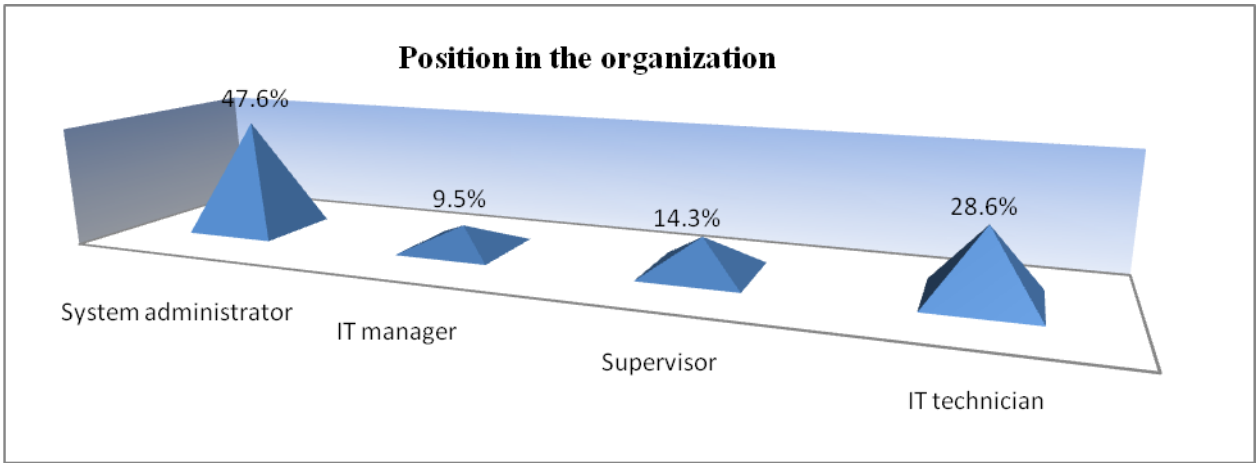


Figure 5.3: Position held

From the findings on the respondents' position in the organization, the study found that most of the respondents as shown by 47.6% indicated that they were system administrators, 28.6% of the respondents indicated that they were IT technicians, 14.3% of the respondents indicated that they were supervisors whereas 9.5% of the respondents indicated that they were IT managers .This was an indication that the levels of management were well represented in the study.

5.3 Information Security

Table 5.3: Information Security Policy

	Percent
Documented	66.7
Approved by management	61.9
Published	47.6
Communicated to ALL employees	57.1
Communicated to all third parties	52.4
No information security	76.2

From the findings on the information security policy in public universities the study found that majority of the respondents as shown by 76.2% indicated that there was no information

security policy, 66.7% indicated that the information security policy was documented, 61.9% indicated that the information security policy was approved by management, 57.1% indicated that the information security policy was communicated to all employees, 52.4% indicated that the information security policy was communicated to all third parties whereas 47.6% indicated that the information security policy was published. This is an indication that there is no information security policy in majority of the state public universities in Kenya.

Table 5.4: Percentage of Employees Aware Of the Information Security Policy

	Frequency	Percent
Less than 10%	6	28.6
Less than 30%	9	42.6
Less than 50%	3	14.3
More than 50%	2	9.5
More than 80%	1	4.8
Total	21	100.0

From the findings on the Percentage of employees aware of the information security policy the study found that most of the respondents as shown by 42.9% indicated that the employees aware of the information security policy were less than 30%, 28.6% indicated less than 10%, 14.3% indicated less than 50%, 9.5% indicated more than 50% whereas 4.8%% indicated more than 80%. This is an indication that in most public universities in Kenya the employees aware of the information security policy were less than 30%.

Table 5.5: Percentage of employees who understands their information system security responsibilities

	Frequency	**Percent**
Less than 10%	4	19.0
Less than 30%	10	47.6
Less than 50%	5	23.8
More than 50%	2	9.5
Total	21	100.0

From the findings on the percentage of employees who understands their information system security responsibilities, the study found that most of the respondents as shown by 47.6% indicated that the employees who understand their information system security

responsibilities were less than 30%, 23.8% indicated less than 50%, 19% indicated less than 10%, whereas 9.5% indicated more than 50%. This is an indication that in most public universities in Kenya less than 30% of the employees understand their information system security responsibilities.

Table 5.6: Information that is considered sensitive/critical in the public universities

	Percent
Student information	66.7
Financial information	81.0
Communication with other universities	76.2
Expansion strategies	71.4

From the findings on the information that is considered sensitive/critical in the public universities the study found that majority of the respondents as shown by 81% indicated that financial information is considered critical, 76.2% indicated communication with other universities, 71.4% indicated expansion strategies whereas 66.7% indicated student information as critical. This is an indication that financial information is the most critical information in the public universities in Kenya.

Table 5.7: Mechanisms used to protect data center from physical access by unauthorized persons in public universities

	Percent
No restriction	42.6
Entry card	57.1
A guard	85.7
Biometrics	52.4
Lock and key	81.0

From the findings on the mechanisms used to protect data center from physical access by unauthorized persons in public universities the study found that majority of the respondents as shown by 85.7% indicated that data centers are protected from physical access by unauthorized persons through guards, 81% indicated lock and key, 57.1% indicated entry card, 52.4% indicated biometrics whereas 42.6% indicated no restriction. This is an

indication that most public universities in Kenya protect data center from physical access by unauthorized persons by use of guards.

Table 5.8: Length of time access rights for an employee who resigns or is dismissed from public universities are revoked

	Frequency	Percent
Some days upon resignation/dismissal	4	19.0
Immediately on receiving resignation/dismissal letter	2	9.5
When he/she clears with the university	9	42.9
As advised by the IT in charge	5	23.8
No policy on revoking rights	1	4.8
Total	21	100.0

From the findings on the length of time access rights for an employee who resigns or is dismissed from public universities are revoked the study found that most of the respondents as shown by 42.9% indicated that access rights for an employee who resigns or is dismissed from public universities are revoked when he/she clears with the university, 23.8% indicated as advised by the IT in charge, 19% indicated some days upon resignation/dismissal, 9.5% indicated immediately on receiving resignation/dismissal letter whereas 4.8% indicated that there are no policies on revoking rights. This is an indication that in most public universities access rights for an employee who resigns or is dismissed are revoked when he/she clears with the university.

Table 5.9: Back up policy in public universities

	Percent
We take daily incremental back ups	61.9
We take daily full back ups	57.1
Weekly full back ups	66.7
Monthly full back ups	76.2
Yearly full back ups	90.5

From the findings on the back up policy in public universities, the study found that majority of the respondents as shown by 90.5% indicated that their universities take yearly full back ups, 76.2% indicated that they take monthly full back ups, 57.1% indicated that they take weekly full back ups, 52.4% indicated that they take daily incremental backups whereas

42.6% indicated that they take daily full back ups. This is an indication that majority of the public universities in Kenya take yearly full back ups. From the findings on whether public universities in Kenya have constituent colleges/campuses, the study revealed that all public universities in Kenya had constituent colleges/campuses as shown by 100%.

Table 5.10: Technologies used to interlink colleges/campuses

	Percent
Digital leased lines	66.7
Analogue leased lines	57.1
VSAT	81
Wireless technology	57.1
GPRS/EDGE (GSM technology)	47.6
Fibre Optic	61.9
Colleges/Campuses not connected	71.4

From the findings on the technologies used to interlink colleges/campuses in public universities, the study found that majority of the respondents as shown by 81% indicated that colleges/campuses are interlinked through VSAT, 71.4% indicated that colleges/campuses are not connected, 66.7% indicated Digital leased lines , 61.9% indicated Fibre Optic, 57.1% indicated wireless technology and analogue leased lines in each case whereas 47.6% indicated GPRS/EDGE (GSM technology). This is an indication that majority of the public universities in Kenya link their campuses through VSAT.

Table 5.11: Mechanism used to protect the network from internet and third parties

	Percent
Access lists	**71.4**
Fire walls	**66.7**
Intrusion detection systems	**57.1**
Strong passwords	**90.5**
Access policies on all terminals	**85.7**
Not sure	**61.9**

From the findings on the mechanism used to protect the university network from internet and third parties, the study found that majority of the respondents as shown by 90.5% indicated

that they protect the network through strong passwords, 85.7% indicated Access policies on all terminals, 71.4% indicated access lists, 66.7% indicated Fire walls, 61.9% were not sure whereas 57.1% indicated intrusion detection systems. This is an indication that majority of the public universities in Kenya protect their networks from internet and third parties through strong passwords.

Table 5.12: Length of time the servers configured to lock automatically lock when not in use

	Frequency	Percent
Not configured to lock out automatically	2	9.5
5 minutes	3	14.3
10 minutes	4	19.0
30 minutes	9	42.9
1 hour	3	14.3
Total	21	100.0

From the findings on the length of time the servers configured to lock automatically lock when not in use, the study found that most of the respondents as shown by 42.9% indicated that the servers take 30 minutes to lock automatically, 19% indicated 10 minutes, 14.3% indicated 5 minutes and 1 hour in each case, whereas 9.5% indicated that the servers were not configured to lock out automatically. This is an indication that in most public universities the servers configured to lock automatically locks after about 30 minutes.

Table 5.13: Length of time the workstations configured to lock automatically

	Frequency	Percent
Not configured to lock out automatically	1	4.8
5 minutes	5	23.8
10 minutes	8	38.1
30 minutes	4	19.0
1 hour	3	14.3
Total	21	100.0

From the findings on the length of time the work stations configured to lock automatically lock when not in use, the study found that most of the respondents as shown by 38.1% indicated that the work stations take 10 minutes to lock automatically, 23.8% indicated 5

minutes, 19% indicated 30 minutes, 14.3% indicated 1 hour whereas 4.8% indicated that the servers were not configured to lock out automatically. This is an indication that in most public universities the work stations configured to lock automatically locks after about 10 minutes.

Table 5.14: Employees Being Sensitized on Information System Security

	Frequency	Percent
Not sensitized	3	14.3
Only once	5	23.8
Regularly	13	61.9
Total	21	100.0

From the findings on how often the employees of public universities are sensitized on information system security, the study found that majority of the respondents as shown by 61.9% indicated that the employees are regularly trained on information system security, 23.8% indicated that the employees are sensitized only once whereas 14.3% indicated that the employees are not sensitized. This is an indication that the employees in public universities are sensitized on information system security regularly.

Table 5.15: Information security policy in universities is reviewed

	Frequency	Percent
Never reviewed	11	52.4
After 3 months	1	4.8
After six months	2	9.5
After one year	3	14.3
After a security incident	4	19.0
Total	21	100.0

From the findings on how often review the information security policy is reviewed in public universities in Kenya, the study found that majority of the respondents as shown by 52.4% indicated that the information security policy is never reviewed, 19% indicated that the information security policy is reviewed after a security accident, 14.3% indicated that the information security policy is reviewed after one year, 9.5% indicated that the information security policy is reviewed after six months whereas 4.8% indicated that the information

security policy is reviewed after 3 months. This is an indication that the information security policy in majority of the public universities in Kenya is never reviewed.

Table 5.16: Policy employed to control access of information in public universities

	Frequency	Percent
PIN number	5	23.8
Entry card	3	14.3
Username and password	12	57.1
Biometrics	1	4.8
Total	21	100.0

From the findings on the policy employed to control access of information in public universities in Kenya, the study found that majority of the respondents as shown by 57.1% indicated that their universities used username and password to control access of information, 23.8% indicated pin number, 14.3% indicated entry card, whereas 4.8% indicated biometrics. This is an indication that majority of public universities in Kenya use username and password to control access of information.

Table 5.17: Policy state about reporting information security events and weaknesses

	Frequency	Percent
No policy on reporting security events	1	4.8
Not sure	3	14.3
Report to ICT	5	23.8
Report to help desk	10	47.6
Write e-mail to all staff	2	9.5
Total	21	100.0

From the findings on what the university's policy state about reporting information security events and weaknesses in public universities in Kenya, the study found that most of the respondents as shown by 47.6% indicated that their universities' policy state that they should report to the help desk, 23.8% indicated they report to ICT, 14.3% indicated they were not sure, 9.5% indicated that they write email to all staff whereas 4.8% indicated that there was no policy on reporting security events.

Table 5.18: Senior management regularly receive reporting

	Frequency	Percent
Yes	12	57.1
No	9	42.9
Total	21	100.0

From the findings on whether senior management regularly receive reporting on the status of information security status or on security incidents, the study found that majority of the respondents as shown by 57.1% indicated that senior management regularly receive reporting on the status of information security status or on security incidents whereas 42.9% indicated that the senior management does not regularly receive reporting on the status of information security status or on security incidents. This is an indication that senior management of public universities regularly receives reporting on the status of information security status or on security incidents.

Table 5.19: Level of agreement that senior management has an appropriate understanding of the importance of information security

	Frequency	Percent
Agree	5	23.8
Neutral	6	28.6
Disagree	10	47.6
Total	21	100.0

From the findings on the level of agreement that senior management has an appropriate understanding of the importance of information security, the study found that most of the respondents as shown by 47.6% disagreed on the statement, 28.6% were neutral on the statement whereas 23.8% agreed on the statement. This is an indication that senior management of public universities in Kenya does not have appropriate understanding of the importance of information security.

Table 5.20: Level of agreement that senior management provide the required level of support for information security

	Frequency	Percent
Agree	2	9.5
Neutral	5	23.8
Disagree	11	52.4
Strongly disagree	3	14.3
Total	21	100.0

From the findings on the level of agreement that senior management provide the required level of support for information security, the study found that majority of the respondents as shown by 52.4% disagreed that senior management provided the required level of support for information security, 23.8% were neutral, 14.3% strongly disagreed whereas 9.5% agreed. This is an indication that senior management of public universities in Kenya does not provide the required level of support for information security. The senior management support has been manifested through policies relating to information security, up to date equipment, provision of funds, trained workforce and supporting employee training program. On the operational structure for security management in public universities in Kenya the study found that in most universities the Top bottom organizational structure is adopted where the orders come from above and should be followed all time. Most do not have information systems security officers and the top most security personnel is a General administrator who gives orders concerning security issues. He/she is mostly assisted by system administrators who supervise the technicians.

Table 5.21: Main approaches taken to manage information security in public universities in Kenya

	Percentage
A structured information security management program or strategy exists	66.7
Security is managed as part of the IT operational plan	51.7
Security is project based	71.4
Security is driven by risk management	61.9
Security is driven by incident management	81.0
Security is primarily guided by security standards	47.6
An ad hoc approach is applied to security	85.7

From the findings on the main approaches that are taken to manage information security in public universities in Kenya, the study found that majority of the respondents as shown by 85.7% indicated that an ad hoc approach is applied to security, 81% indicated that security is driven by incident management, 71.4% indicated that security is project based, 66.7% indicated that structured information security management program or strategy exists, 61.9% indicated that security is driven by risk management, 51.7% indicated that security is managed as part of the IT operational plan whereas 47.6% indicated that security is primarily guided by security standards. This is an indication that the public universities in Kenya manage information security using various approaches.

Table 5.22: Level of agreement that current management approach is effective

	Frequency	Percent
Agree	3	14.3
Neutral	4	19.0
Disagree	12	57.1
Strongly disagree	2	9.5
Total	21	100.0

From the findings on the level of agreement that current management approach adopted by public universities in Kenya prove to be effective in terms of achieving security requirements, the study found that majority of the respondents as shown by 57.1% disagreed that the current management approach adopted by their organization prove to be effective in terms of achieving security requirements, 19% were neutral, 14.3% agreed whereas 9.5% strongly disagreed. This is an indication that current management approach adopted by public universities in Kenya prove to be ineffective in terms of achieving security requirements.

On the changes required to improve the effectiveness of information security management approach in public universities the study found that the changes would include management change, changes in the organizational structure, adoption of a corporate culture, increased delegation, formulation of inclusive policies, and open recruitment process. The study found that the standards have been useful in helping with the management of information security in public universities in Kenya through improved security policies, quality services by IT

firms, qualified staff who are trained to meet the required standards and up to date technology.

Table 5.23: Level of agreement on security policy development and implementation

	Frequency	Percent
Agree	4	19.0
Neutral	6	28.6
Disagree	11	52.4
Total	21	100.0

From the findings on the level of agreement that security policy development and implementation result in the required level of involvement and support from relevant technical stakeholders, the study found that majority of the respondents as shown by 52.4% disagreed that the security policy development and implementation result in the required level of involvement and support from relevant technical stakeholders, 28.6% were neutral, whereas 19% agreed. This is an indication that security policy development and implementation in the public universities in Kenya result in the required level of involvement and support from relevant technical stakeholders.

Table 5.24: Level of agreement that on how public universities treat security policies

	Frequency	Percent
Agree	10	47.6
Neutral	8	38.1
Disagree	3	14.3
Total	21	100.0

From the findings on the level of agreement that public universities treat security policies as an essential component of managing information security, the study found that most of the respondents as shown by 47.6% agreed that their institutions treat security policies as an essential component of managing information security, 38.1% were neutral, whereas 14.3% disagreed. This is an indication that public universities in Kenya treat security policies as an essential component of managing information security. On the awareness activities undertaken by the public universities in Kenya the study found that they include training the system administrators and students on how to handle security issues, verification procedures

on information, identification checks or searches on employees, cyber security awareness day for the employees, developing a website where people can discuss security issues, and organizing computer classes on security for the students.

Table 5.25: Security Awareness an Activity an Important Priority in Public University

	Frequency	Percent
Yes	8	38.1
No	13	61.9
Total	21	100.0

From the findings on whether raising security awareness an activity that is given an important priority in the public universities in Kenya, the study found that majority of the respondents as shown by 61.9% indicated that raising security awareness is not given an important priority in their institution whereas 38.1% indicated that raising security awareness is given an important priority in their organization. This is an indication that raising security awareness is not given an important priority in the public universities in Kenya. The study found that the events or situations that have resulted in an outcome that has been very effective in raising security awareness in public universities the study found the activities to be crushing of computers, slow speed of the computers, loss of data, manipulation of university data and cracking of security codes.

Table 5.26: Level of agreement on the existing security activities

	Frequency	Percent
Agree	4	19.0
Neutral	7	33.3
Disagree	10	47.6
Total	21	100.0

From the findings on the level of agreement that the existing security activities that are currently undertaken by public universities in Kenya adequately address requirements for security awareness in public universities, the study found that most of the respondents as shown by 47.6% disagreed that the existing security activities that are currently undertaken adequately address requirements for security awareness, 33.3% were neutral, whereas 19%

agreed. This is an indication that the existing security activities that are currently undertaken by public universities in Kenya do not adequately address requirements for security awareness. If security awareness is below the level that it should be, the study found that it can be addressed through personnel training, increased staffing in the security department, organizing talks on security issues and increased management support in terms of resources.

Table 5.27: Culture of Compliance' Towards Information Security

	Frequency	Percent
Yes	7	33.3
No	14	66.7
Total	21	100.0

From the findings on whether a 'culture of compliance' towards information security is reflected through public university's work practices and business processes, the study found that majority of the respondents as shown by 66.7% indicated that a 'culture of compliance' towards information security is not reflected through their institution's work practices and business processes whereas 33.3% indicated that a 'culture of compliance' towards information security is reflected through the institution's work practices and business processes. This is an indication that a 'culture of compliance' towards information security is not reflected through public university's work practices and business processes.

Table 5.28: Public universities are well-positioned to 'detect and defend' against security incidents

	Frequency	Percent
Yes	8	38.1
No	13	61.9
Total	21	100.0

From the findings on whether public universities in Kenya are well-positioned to 'detect and defend' against security incidents, the study found that majority of the respondents as shown by 61.9% indicated that their institutions are not well-positioned to 'detect and defend' against security incidents whereas 38.1% indicated that that their institutions are well-positioned to 'detect and defend' against security incidents. This is an indication that public

universities in Kenya are not well-positioned to 'detect and defend' against security incidents.

Table 5.29: Main causes of Security Incidents in Public Institutions

	Percentage
Viruses and malicious software	90.5
Cyber or internal based attacks	61.9
System or software errors	81.0
System administrator errors or non-compliance	66.7
User errors or non-compliance	76.2
Hardware failure	85.7
Environmental failure	57.1
Students riots	71.4

From the findings on the main causes of Security Incidents in Public universities in Kenya, the study found that majority of the respondents as shown by 90.5% indicated the main cause of Security Incidents in their institution as viruses and malicious software, 85.7% indicated Hardware failure, 81% indicated system or software errors, 76.2% indicated system administrator errors or non-compliance, 71.4% indicated students riots, 66.7% indicated system administrator errors or non-compliance, 61.9% indicated cyber or internal based attacks whereas 57.1 indicated environmental failure. This is an indication that there are many causes of Security Incidents in Public universities in Kenya. The study found that the current security issues facing public universities are inadequate training, complicated hardware, virus and malware infections, lack of management attention to security issues, slow investigation process and poorly chosen passwords. On the new security technologies or other measures to increase compliance the universities are considering over the next 1 to 2 years, the study found them to be supplementing the IT security system, development of an IT risk management program, networking the computers in the IT departments of campuses, and outsourcing IT experts to develop a good system.

Table 5.30: Barriers or obstacles to achieving improved security compliance in public universities in Kenya

	Percentage
Funding and Resourcing	71.4
Awareness and understanding	76.2
'Culture of Compliance' (work practices and business processes)	66.7
Technology Deficiencies (lack of or inadequate)	85.7
Incident detection and response capability	81.0
Clear Direction in Security Governance	61.9
Organizational Commitment and Support	57.1
Inadequate Industry Security Standards	52.4
Capacity to measure effectiveness or value of security	71.4
Capacity to measure effectiveness or value of security	66.7

From the findings on the main barriers or obstacles to achieving improved security compliance in public universities in Kenya, the study found that most of the respondents as shown by 85.7% indicated the main barrier to achieving improved security compliance in their institution as Technology Deficiencies, 81% indicated Incident detection and response capability, 81% indicated system or software errors, 76.2% indicated awareness and understanding, 71.4% indicated capacity to measure effectiveness or value of security and Funding and Resourcing in each case , 66.7% indicated culture of compliance and Capacity to measure effectiveness or value of security in each case, 61.9% indicated clear direction in Security Governance Organizational Commitment and Support, 57.1% indicated organizational commitment and Support whereas 52.4% indicated inadequate industry Security Standards. This is an indication that there are many barriers or obstacles to achieving improved security compliance in public universities in Kenya.

Table 5.31: Whether public universities in Kenya carry out information security audit

	Frequency	Percent
Yes	5	23.8
No	16	76.2
Total	21	100.0

From the findings on whether public universities in Kenya carry out information security audit, the study found that majority of the respondents as shown by 76.2% indicated that their

institutions do not carry out information security audit whereas 23.8% indicated that their institutions carry out information security audit. This is an indication that public universities in Kenya do not carry out information security audit.

The critical success factors for the successful management of information security in public universities in Kenya were found to be security awareness and training, management support, balanced budget, information security policy enforcement and organization mission.

5.4 Regression Analysis

In this study, a multiple regression analysis was conducted to test the influence among predictor variables. The research used Statistical Package for Social Sciences (SPSS V 20) to code, enter and compute the measurements of the multiple regressions

Table 5.32: Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.969[a]	.939	.921	.01575

Adjusted R squared is coefficient of determination which tells us the variation in the dependent variable due to changes in the independent variable. From the findings in the above table, the value of adjusted R squared was 0.969, an indication that there was variation of 92.1% on the information security systems in universities dues to changes in software management, psychical management, information security policy and I.S audit and asset management at 95% confidence interval . This shows that 92.1% changes in information security systems in universities could be accounted to changes in software management, psychical management, information security policy and I.S audit and asset management. R is the correlation coefficient which shows the relationship between the study variables. The findings show that there was a strong positive relationship between the study variables as shown by 0.969.

Table 5.33: ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	0.002	2	.001	3.869	.015[b]
	Residual	0.609	29	.021		
	Total	0.611	31			

From the ANOVA statistics in table above, the processed data, which is the population parameters, had a significance level of 1.5 which shows that the data is ideal for making a conclusion on the population's parameter as the value of significance (p-value) is less than 5%. The calculated was greater than the critical value (2.262 <3.869) an indication that information security systems in universities significantly changes due to changes in software management, psychical management, information security policy and I.S audit and asset management. The significance value was less than 0.05 an indication that the model was statistically significant.

Table 4.34: Coefficients

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	.455	.231		1.973	.106
	Software Management	.016	.009	.444	1.815	.009
	Psychical Management	.182	.050	1.231	3.616	.036
	Information Security Policy	.053	.017	1.075	3.159	.025
	I.S audit and asset management	.204	.240	.230	.850	.028

From the data in the above table the established regression equation was

$Y = 0.455 + 0.016 X_1 + 0.182 X_2 + 0.053 X_3 + 0.204 X_4$

From the above regression equation it was revealed that software management, psychical management, information security policy and I.S audit and asset management to a constant zero , information security systems in universities would stand at 0.455 , a unit increase in software management would lead to increase in information security systems in universities by a factor of 0.016, unit increase in physical management would lead to increase in information security systems in universities by a factor of 0.182 , a unit increase in information security policy would lead to increase in information security systems in universities by a factor of 0.053 and unit increase in I.S audit and asset management would lead to increase in in information security systems in universities by a factor of 0.204.

CHAPTER SIX:

THE PROPOSED UNIVERSITY INFORMATION SYSTEMS SECURITY FRAMWORK

6.1 Introduction

The first step in creating a secure information system is to identify threats. Once potential problems are known, the second step, establishing controls, follows. Finally, the third step consists of audits to discover any breach of security. Threats include computer crime and abuse, human error, natural disasters, hardware and software failures. Controls include general and application controls while auditing includes both system operational audits and financial audits. While both the conceptual and the developed framework generally follow this approach, the developed framework considers and is in line with Kenyan public universities management approach.

6.2 Justification for the developed Frame work.

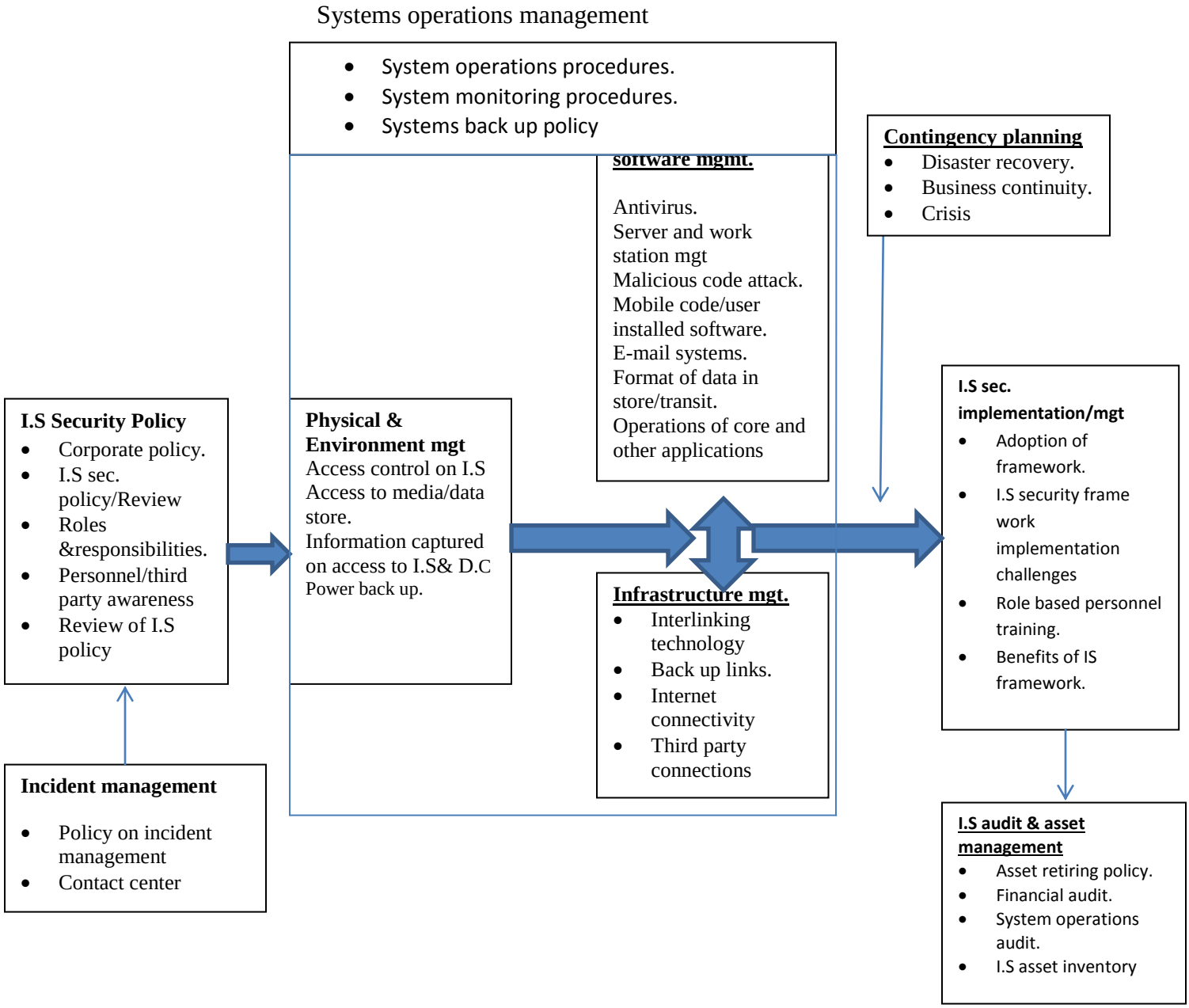
Although the developed frame work is mainly derived from literature review, results from the research supports it in a number of cases. The research not only confirms that majority of the universities do not have information security policy but that senior university management do not have appropriate understanding of the importance of information security. This could explain why most respondents feel that the management have not provided the required level of support for information security and that the current management to security is not effective. The research also shows that an ad hoc approach is applied as the main approach taken to manage information security in Kenyan public universities.

since most of the universities adopt and follow a top bottom organizational structure, it was necessary to develop a frame work in line with this structure if it has to be adopted. Furthermore, the developed frame work can also be used in other government corporations most of which adopt similar organizational structure.

6.3 Validation of the Frame work.

Validation of the frame works was done by developing the questionnaire, the main data collection tool in the research, based on the frame work elements. A copy of the questionnaire is attached at the appendix.

6.4: Proposed Conceptual Model for Increased Adoption of Information Security Architecture



Information systems security policy; Each university should have a policy to manage its information, whether electronic or hard copy. Appropriately securing university information will not only protect it against consequences of breaches of confidentiality but also lead to failures of integrity and interruptions to the availability of that information. Such policy must be ratified by the organization to form part of its policies and procedures which includes regulations for conduct. The policy must be communicated to and must be applicable to all staff, students and other relevant parties. To ensure compliance, terms and conditions of employment and the organization's code of conduct should set out all employees and students responsibilities with respect to the use of computer systems and all sets of data, computer based or otherwise. This would ensure that all members comply or face disciplinary action. The policy needs to be in line with the corporate policy, be reviewed, stipulate roles and responsibilities and be communicated to staff, students and relevant third parties. policy on incident management including a decision on contact center is also a decision that must be made by top university management.

Physical and environment control; policy level then leads to the systems operations module. Of great concern is the physical control of access to information. This module concerns not only protection of the system's physical equipment but also related software and interlinking hardware. Equipment supporting systems must be planned to have adequate processing power, storage and network capacity available for both current and projected needs, appropriate levels of resilience and fault tolerance. Areas and offices where confidential or restricted information resides must be given appropriate physical security and access control and staff in such areas trained on potential security risks and measurers to control them. systems operations must be so well managed that it clearly handles issues like proper registration and identification of all system users, proper management of access including the university e-mail system, network segregation and use of configured firewalls , subjecting remote access to robust authentication, security event logs, operational audit logs and error

logs, all of which must be managed and reviewed by qualified staff. proper back up of the organizations information and the ability to recover them should an attack occur is an important priority at systems operation level.

Contingency planning; should there be any form of attack on the system, measurers must be put in place to ensure recovery and business continuity. Safeguards must be put in place to protect the integrity of information during recovery and restoration of data files. There must be a continuation plan for each system or activity consistent with the university overall contingencies and plans.

Information systems security implementation and management; having developed an appropriate security policy with express authority from the university chief executive(vice-chancellor), implementation should have fewer challenges. the vice-chancellor takes ownership of the systems security policy and ensures availability of sufficient training and information material for all users to enable them protect data and information systems. This module handles role based training to equip personnel charged with various responsibilities concerning security of university information, adoption and benefits of the framework and implementation challenges in adopting the information security frame work.

Information systems audit and asset management; this module concerns not only the retirement of IT assets but also the audit of systems operations and consequential financial audits. Not only an inventory of all important assets associated with information systems be documented and maintained but also an identification and documentation of rules for acceptable use information systems. owners and custodians of such information must be designated for all assets associated with information.

CHAPTER SEVEN:

CONCLUSION AND FURTHER WORK

7.1 Introduction

From the analysis and data collected, the following summary of findings, conclusions and recommendations were made. The responses were based on the objectives of the study. The researcher had intended to establish the challenges faced by public universities in adopting and implementing information systems security frameworks, develop a conceptual information systems security framework suitable for Kenya public universities and to assess the level of information systems security compliance if the Kenyan public universities were to adopt the suggested framework.

7.2 Achievements

The research study has successfully investigated the level of preparedness in dealing with information systems security threats in Kenya public universities.

Table 7.35 : Mapping Objectives into Research Questions

	Objectives	**How they were achieved**
1	to establish the challenges faced by public universities in adopting and implementing information systems security frameworks	Literature review, Questionnaires
2	To develop a conceptual information systems security framework suitable for Kenya public universities	Literature review Questionnaires,
3	to assess the level of information systems security compliance if the Kenyan public universities were to adopt the suggested framework	Literature review Questionnaires,

7.3 Summary of Findings

From the findings on the information security policy in public universities the study found that there was no information security policy in public universities as shown by 76.2%, the

information security policy was documented, against the information security policy was approved by management, the information security policy was communicated to all employees, the information security policy was communicated to all third parties and the information security policy was published.

The study found that less than 30% of the employees in public universities in Kenya are aware of the information security policy and understand their information system security responsibilities. From the findings on the information that is considered sensitive/critical in the public universities the study found that financial information is considered sensitive/critical as shown by 81%, against communication with other universities, expansion strategies and student information as critical.

From the findings on the mechanisms used to protect data center from physical access by unauthorized persons in public universities the study found that centers are protected from physical access by unauthorized persons mainly through guards as shown by 85.7%, compared to lock and key, entry card, and biometrics. From the findings on when access rights for an employee who resigns or is dismissed from public universities are revoked the study found that access rights for an employee who resigns or is dismissed from public universities are revoked when he/she clears with the university (42.9%), compared to as advised by the IT in charge, some days upon resignation/dismissal, and immediately on receiving resignation/dismissal letter. From the findings on the back up policy in public universities, the study found that universities take yearly full back ups (90.5%), monthly full back ups, weekly full back ups, daily incremental backups and daily full back ups.

The study revealed that all public universities in Kenya had constituent colleges/campuses as shown by 100%. The study found that the technologies that link colleges/campuses in public universities in Kenya include VSAT, Digital leased lines, Fibre Optic, wireless technology and analogue leased lines and GPRS/EDGE (GSM technology). From the findings on the mechanism used to protect the university network from internet and third parties, the study found that public universities in Kenya protect their networks through strong passwords (57.1%), access policies on all terminals, access lists, Fire walls and intrusion detection systems.

From the findings on the length of time the servers configured to lock automatically lock when not in use, the study found that most of the respondents as shown by 42.9% indicated that the servers take 30 minutes to lock automatically, 19% indicated 10 minutes, 14.3% indicated 5 minutes and 1 hour in each case, whereas 9.5% indicated that the servers were not configured to lock out automatically. The study found that in most public universities the work stations configured to lock automatically locks after about 10 minutes.

The study found that the employees in public universities are sensitized on information system security regularly. The study found that the information security policy in majority of the public universities in Kenya is never reviewed. The study found that public universities in Kenya used username and password as shown by 57.1% to control access of information, pin number, entry card and biometrics. The study found that public universities in Kenya have security policies that state that employees should report to the help desk, report to ICT, and write email to staff.

The study found that senior management of public universities in Kenya regularly receives reporting on the status of information security status or on security incidents. The study found that senior management of public universities in Kenya does not provide the required level of support for information security. The senior management support has been manifested through policies relating to information security, up to date equipment, provision of funds, trained workforce and supporting employee training program. On the operational structure for security management in public universities in Kenya the study found that in most universities the Top bottom organizational structure is adopted where the orders come from above and should be followed all time. Most do not have IT managers and the top most security personnel is a General Manager who gives orders concerning security issues. He/she is mostly assisted by system administrators who supervise the technicians.

From the findings on the main approaches that are taken to manage information security in public universities in Kenya, the study found that an ad hoc approach is applied to security as shown by 85.7%, security is driven by incident management, security is project based, Digital leased lines, structured information security management program or strategy exists,

security is driven by risk management, security is managed as part of the IT operational plan whereas security is primarily guided by security standards.

The study found that the current management approach adopted by public universities in Kenya prove to be ineffective in terms of achieving security requirements. On the changes required to improve the effectiveness of information security management approach in public universities the study found that the changes would include management change, changes in the organizational structure, adoption of a corporate culture, increased delegation, formulation of inclusive policies, and open recruitment process. The study found that the standards have been useful in helping with the management of information security in public universities in Kenya through improved security policies, quality services by IT firms, qualified staff who are trained to meet the required standards and up to date technology.

The study found that security policy development and implementation in the public universities in Kenya result in the required level of involvement and support from relevant technical stakeholders. The study found that public universities in Kenya treat security policies as an essential component of managing information security. On the awareness activities undertaken by the public universities in Kenya the study found that they include training the system administrators and students on how to handle security issues, verification procedures on information, identification checks or searches on employees, cyber security awareness day for the employees, developing a website where people can discuss security issues, and organizing computer classes on security for the students.

The study found that raising security awareness is not given an important priority in in the public universities in Kenya. The study found that the events or situations that have resulted in an outcome that has been very effective in raising security awareness in public universities the study found the activities to be crushing of computers, slow speed of the computers, loss of data, manipulation of university data and cracking of security codes. The study found that the existing security activities that are currently undertaken by public universities in Kenya do not adequately address requirements for security awareness. If security awareness is below the level that it should be, the study found that it can be addressed through personnel

training, increased staffing in the security department, organizing talks on security issues and increased management support in terms of resources.

The study found that a 'culture of compliance' towards information security is not reflected through public university's work practices and business processes. The study found that the public universities in Kenya are not well-positioned to detect and defend against security incidents.

The study found that there are many causes of Security Incidents in Public universities in Kenya. The study found that the current security issues facing public universities are inadequate training, complicated hardware, virus and malware infections, lack of management attention to security issues, slow investigation process and poorly chosen passwords. On the new security technologies or other measures to increase compliance the universities are considering over the next 1 to 2 years, the study found them to be supplementing the IT security system, development of an IT risk management program, networking the computers in the IT departments of campuses, and outsourcing IT experts to develop a good system.

The study found that the main barriers to achieving improved security compliance in public universities in Kenya to be technology Deficiencies , Incident detection and response capability, system or software errors, awareness and understanding, capacity to measure effectiveness or value of security and Funding and Resourcing in each case ,culture of compliance and Capacity to measure effectiveness or value of security in each case, clear direction in Security Governance Organizational Commitment and Support, organizational commitment and Support and inadequate industry Security Standards. The study found that public universities in Kenya do not carry out information security audit. The critical success factors for the successful management of information security in public universities in Kenya were found to be security awareness and training, management support, balanced budget, information security policy enforcement and organization mission.

7.4 Conclusions

The study concludes that that there is no information security policy in most public universities in Kenya and the universities need to come up with security policies which will ensure safety of information. The study concludes that very few employees in public universities in Kenya are aware of the information security policy in the university and understand their information system security responsibilities. The study concludes that financial information is the most critical information in public universities.

The study concludes that data centers in the public universities should be protected from physical access by unauthorized persons through guards, lock and key, entry card and biometrics. The study concludes that access rights for an employee who resigns or is dismissed from public universities are usually revoked when the employee clears with the university which may lead to information loss as the clearing may take some time.

The study concludes that all public universities in Kenya have constituent colleges/campuses linked through different technologies like VSAT, Digital leased lines, Fibre Optic, wireless technology and GSM technology.

The study concludes that public universities in Kenya usually protect their networks from third parties through various safety mechanisms like strong passwords and access policies on terminals. The study concludes that in most public universities the work stations and servers are configured to lock automatically and locks after some time hence exposing the university to the risk of data manipulation and access by third parties.

The study concludes that the employees in public universities are sensitized on information system security regularly with the information security policy not reviewed. The study concludes that senior management of public universities in Kenya does not provide the required level of support for information security in the universities. The public universities in Kenya have a rigid organizational structure where the employees follow orders without questioning. This has led to poor information security policies due to lack of innovation and employee empowerment.

The study concludes that public universities in Kenya have adopted various approaches in information security management. An adhoc approach is usually applied to security in

majority of the universities. The study also concludes that the management approaches adopted by public universities in Kenya are ineffective in terms of achieving security requirements. The study concludes that security policy development and implementation in the public universities in Kenya result in the required level of involvement and support from relevant technical stakeholders. The study also concludes that the public universities in Kenya undertake security awareness activities in order to enhance information security in the universities.

The study concludes that raising security awareness is not given an important priority in in the public universities in Kenya. There have been events or situations that have resulted in an outcome that has been very effective in raising security awareness in public universities in Kenya. Some include crushing of computers, loss of data, manipulation of university data and cracking of security codes. The study concludes that the existing security activities that are currently undertaken by public universities in Kenya do not adequately address requirements for security awareness.

The study concludes that the public universities in Kenya are not well-positioned to detect and defend against security incidents. The study concludes that public universities in Kenya are faced with security issues like inadequate training, complicated hardware, virus and malware infections, lack of management attention to security issues, slow investigation process and poorly chosen passwords. The study concludes that there are many barriers to achieving improved security compliance in public universities in Kenya with technology deficiencies as the major barrier.

The study concludes that public universities in Kenya do not carry out information security audit. The critical success factors for the successful management of information security in public universities in Kenya were found to be security awareness and training, management support, balanced budget, information security policy enforcement and organization mission

7.5 Limitation of the Study and Suggestions for Future Research

In the process of conducting this study, it encountered a number of limitions some of which offer opportunities for future research. The duration of the study was not long enough to

enable a proper investigation of the responses and survey, therefore the results may suffer from internal validity threats. Majority of the respondents were IT employees who may not have the final authority in making decision to information security. Since the study is solely conducted in IT department of public universities, the results may suffer from industrial biases. Therefore the results needs to be interpreted carefully and repricated in other organizations to improve their relevance. further more, this research is more of a general survey on all aspects of systems security.

The results of this study suggest new directions for future research. Researchers in the field of information system ought to put more emphasis on information security management factors rather than status of information security. Further research therefore to put more emphasis on IS security as an administrative tool rather than a technological innovation. Furthermore an in-depth study is required to rationalize the security factors. Researchers need to establish issues with specific aspects of date security e.g. data integrity or availability as more and more of the universities adopt online services delivery to current and potential students.

7.6 Recommendations

The study recommends that public universities train the system administrators and students on how to handle security issues, verify procedures on information, carry out identification checks or searches on employees, organize cyber security awareness day for the employees, develop a website where people can discuss security issues, and organize computer classes on security for the students.

The study recommends that the public universities in Kenya supplement their current IT security system, develop an IT risk management program, and outsource IT experts to develop a good security system. As much as they may not avoid outsourcing, universities need to develop sound contractual agreements to ensure that contractors and consultants keep confidence.

The study recommends that the public universities conduct regular audits on their Information security systems in order to identify whether the security functionalities put in place are working as intended and hence support the organizations to accomplish their goals.

Most universities have an IT director as the senior most IT personnel. The study recommends that all the IT directors have information systems security training before being hired or have information systems security training upon employment. Better still, each university needs to create the position of information systems security officer to deter personnel that may attempt to use the computer as a tool to commit crime.

GLOSSARY OF IMPORTANT WORDS

Asset-In the context of ISO 27001 and ISO 27002, an asset is any tangible or intangible thing that has value to an organization.

Attack- a human who exploits vulnerability perpetrates an attack on the system. An attack can be launched by another system as when one system sends an overwhelming set of messages to another virtually shutting down the second system's ability to function.

Availability -Availability is a characteristic that applies to assets. An asset is *available* if it is accessible and usable when needed by an authorized entity. *Assets* include things like information, systems, facilities, networks, and computers. All of these assets must be available to authorized entities when they need to access or use them.

Confidentiality-Confidentiality is a characteristic that applies to information. To protect and preserve the *confidentiality* of information means to ensure that it is not made available or disclosed to unauthorized entities. In this context, entities include both individuals and processes.

Control-A *control* is any administrative, management, technical, or legal method that is used to manage risk. *Controls* are safeguards or countermeasures. Controls include things like practices, policies, procedures, programs, techniques, technologies, guidelines, and organizational structures.

E-government-term generally used to describe the delivery of services via network technologies to citizens, business and government agencies, it involves a comprehensive use of ICTs to support the business processes that a government performs, typically the provision of information and services.

Government Corporation-this is legal entity created by a government to undertake commercial activities on behalf of the owner government, the term parastatals may sometimes be used.

Information security-Information security is all about protecting and preserving information. It's all about protecting and preserving the confidentiality, integrity, authenticity, availability, and reliability of information.

Information security event -An *information security event* indicates that the security of an information system, service, or network may have been breached or compromised. An information security event indicates that an **information security policy** may have been violated or a safeguard may have failed.

Information security incident-An *information security incident* is made up of one or more unwanted or unexpected information security events that could very likely compromise the security of your information and weaken or impair your business operations**.**

Information security management system (ISMS)-An *information security management system (ISMS)* includes all of the policies, procedures, plans, processes, practices, roles, responsibilities, resources, and structures that are used to protect and preserve information. It includes all of the elements that organizations use to manage and control their information security risks. An ISMS is part of a larger *management system*.

Information security policy- *information security policy* statement expresses management's commitment to the implementation, maintenance, and improvement of its information security management system.

Information Systems-this is a discrete set of information resources organized expressedly for collection, processing, maintenance, use, sharing or disposition of information

Information Systems Security-protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users, including those measurers necessary to detect, document, and counter such threats.

Malicious Code-Collective term for program code or data that is intentionally included in or inserted into an information system for unauthorized purposes without the knowledge of the user. Examples include viruses, logic bombs, Trojan horses and worms.

Policy-A *policy* statement defines a general commitment, direction, or intention. An *information security policy* statement expresses management's commitment to the implementation, maintenance, and improvement of its information security management system.

Public servant- Any employee of the state, whether in a temporary or permanent capacity, and any other person performing a government function, including, but not limited to, a consultant, contractor, advisor or a member of a temporary commission.

Risk-The concept of *risk* combines three ideas: it selects an event, and then combines its probability with its potential impact. It asks two questions: what is the probability that a particular event will occur in the future? And what negative impact would this event have if it actually occurred? So, a *high risk event* would have both a high probability of occurring and a big negative impact if it occurred. The concept of *risk* is always future oriented: it worries about the impact events could have in the future.

Public university- public university means a university established and maintained out of public funds

Risk analysis-Risk analysis uses information to identify possible sources of risk. It uses information to identify threats or events that could have a harmful impact. It then estimates the risk by asking: what is the probability that this event will actually occur in the future? And what impact would it have if it actually occurred?

Risk assessment-A *risk assessment* combines two techniques: a risk analysis and a risk evaluation.

Risk evaluation-A *risk evaluation* compares the estimated **risk** with a set of risk criteria. This is done in order to determine how significant the risk really is. The estimated risk is established by means of a **risk analysis**.

Security Policy-A written principle or course of action adopted by a corporation to ensure that its security affairs are conducted effectively.

Standard-A *standard* is a document. It is a set of rules that control how people develop and manage materials, products, services, technologies, tasks, processes, and systems.

System Assets- Information, hardware, software and services required to support the business of the corporation, and identified during the risk assessment process as assets that need to be protected.

Third party- In the context of a specific issue, a *third party* is any person or body that is recognized as independent of the people directly involved with the issue in question.

Threats-any circumstance or event with the potential to adversely impact organizational operations(including mission, functions, image or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destructions, disclosure, modification of information and/or denial of service.

Vulnerability-is a weakness in the security system e.g. in the procedures, design or implementation, that might be exploited to cause loss or harm.

REFERENCES

1 Briggs L., *Shoring up your framework*, esj.com, 2007, retrieved, 20th November 2012,<http://esj.com/articles/2007/07/17/shoring-up-your-framework.aspx>

2 Daily Nation, , '*internet frauds cost Kenya 3 billion'*, nation.co.ke, Tuesday October 18, 2012, retrieved 18th October,2011

<http://www.nation.co.ke/business/news/internet+fraud+costs+kenya+banks+shs3bn/-/1006/1156190/-/wk853xz/-index.html.>

3 Dhillon,G.,*Principles of information systems: Text and cases*. Wiley and sons, 2007

4 E-government 2004, 'E-government priorities and implementation framework', *E-government Strategy; the strategic framework, Administrative structure, training requirements and standardization Framework*, 2004, pp4-15.

5 Maliokis, A., and Mylonokis J., *Identifying and managing enterprise security risks in online business convergence environments*, macrothink.org, Vol. 1, No. 1, July 2010 retrieved 12, October, 2012.

<http://www.macrothink.org/journal/index.php/bms/article/view/350>

6 Michael Kimwele, Waweru Mwangi, Stephen Kimani, 'Adoption of information technology security Policies: case study of Kenyan small and medium enterprises (SMES*)', Journal of Theoretical and Applied Information Technology*, Vol18, 2010,
Retrieved 11 October 2012,
<http://www.jatit.org/volumes/research-papers/Vol18No2/1Vol18No2.pdf>

7 MIGA and the Africa region of the World Bank, *Privatization in Kenya. Country Fact sheet*. fdi.net, August 2001; retrieved December 2, 2012.
<http://www.fdi.net/documents/WorldBank/databases/plink/factsheets/kenya.htm>

8 Mwaura, K., 'E-government good for Kenya, But are we equal to the task?' *Saturday Nation*. February, 23, 2008, pp.11.

9 Nduati, L., 'Massive cyber attack hits 100 state websites', *Daily Nation*, January 18, 2012, pp.1-2.

10 Peterson Obara Magutu, Joel Kiplagat Lelei, jklelei, Charles M. Borura, *Information systems implementation in state parastatals*, journal.aibuma.org, Vol. 1April 13, 2010, retrieved on 14th October 2012

<http://journal.aibuma.org/Paper16_IS_Implementation_in_State_Corporations.pdf>

11 Pfleeger C.P, Pfleeger S.L., *Security in computing*, Pearson Education Inc. , 2007

12 Ponemon institute, 2010 *Annual Study: U.S. Cost of a Data Breach*, msisac.cisecurity.org, 2011. Retrieved on2 February 2012. <http://msisac.cisecurity.org/resources/reports/documents/symantec_ponemon_data_breach_costs_report2010.pdf>

13 Robb, C. , *Desperately seeking security frameworks- a road map for state CIOs*, nascio.org, March 2009, retrieved 20th September, 2012

<www.nascio.org/publications/.../NASCIO-SecurityFrameworks.pdf>

14 Schweitzer, J. A., *Managing information security-administrative, electronic and legal measurers to protect business information*, 2nd Edition, Butterworth publishers, 1990

15 Stoneburner G., *Underlying technical models for information technology security*., csrc.nist.gov, NIST special publication 800-33, 2001, retrieved on 23 October 2012,

<http://csrc.nist.gov/publications/nistpubs/800-33/sp800-33.pdf>

16 Wanjiku,R, '*Kenya works on training information security managers'*,agonoconsulting.com, 2008, retrieved on5th November,2008. http://www.aganoconsulting.com/businessnews/archives/18

17 Wohlever K., *Information Security Framework*, osc.edu, OSC-3, 05/27/2009, retrieved on 20 october 2012,

<Http://www.OSC.edu/supercomputing/policies/docs/OSC%20Information%20Framework%20-%20OSC%20OSC%203v2.pdf.>

18 Juma P. "*Hackers blamed in KU exam row",* Daily Nation, 02/12/2011. < *www.nation.co.ke/News/Hackers-blamed-in.../-/index.html*>

19 Ombati C. & Kamau M. "*No breakthrough in hacked police site*" standard digital, retrieved on 13/02/2013. http://www.standardmedia.co.ke/?id=2000026119&cid=4&articleID=2000026119

20 Rodrigues A.J, ICT Research Capacity: Challenges & Strategies in Kenya, EuroAfrica-ICT Awareness Workshop. 2nd -3rd March2009, retrieved on 23rd, May, 2013. euroafrica-**ict**.org.sigma-orionis.com/downloads/rwanda/Rodriques.pdf

Appendix 1

List of the Kenyan Public universities by June 2013

Sno	University name	Area	University status	Original name	Year established	Campus	Website
1	University of Nairobi	Nairobi	1970	Royal Technical College, Royal College Nairobi	1956	Main campus, Kikuyu campus, Chiromo campus, Lower Kabete campus, Upper Kabete Campus, Parklands law school,Embu Univ. college Embu, South Eastern Univ. College Kitui, Kisumu campus	http://www.uonbi.ac.ke/
2	Moi University	Eldoret	1984	Moi University	1984	CONSTITUENT COLLEGES: Garissa University College, Rongo University College, CAMPUSES: Odera Akang'o yala campus, Mombasa Campus, Kericho Campus, Kitale Campus, Alupe Campus, Nairobi Campus,	http://www.mu.ac.ke/
3	Kenyatta University	Nairobi	1985	Kenyatta University College	1965	Main campus, Parklands campus, Ruiru campus, City campus, Kitui campus, Mombasa campus, Nakuru campus,Pwani University College, Machakos University	http://www.ku.ac.ke/

						College	
4	Egerton University	Njoro	1988	Egerton Farm School, Egerton Agricultural College	1939	Kisii university college and Laikipia university college	http://www.egerton.ac.ke/
5	Maseno University	Maseno	1991	Maseno Govt. Training Institute, Siriba Teachers College	1955	Oginga Odinga University	http://maseno.ac.ke/
6	Jomo Kenyatta University of Agriculture and Technology	Nairobi	1994	Jomo Kenyatta College of Agriculture	1981	Multimedia University College of Kenya, Meru University College of Science and Technology,	http://www.jkuat.ac.ke/
7	Masinde Muliro University of Science and Technology	Kakamega	2009	Western College of Arts and Applied Sciences	1972		http://www.mmust.ac.ke/
8	Dedan Kimathi University of Technology	Nyeri	2012	Kimathi Institute of Technology, Kimathi University College of Technology(2007)as a Constituent College of Jomo Kenyatta University of Agriculture and Technology	1972	Main Campus, Nyeri	http://www.dkut.ac.ke/
9	Chuka University	Chuka	2012	Egerton University Eastern Campus College,Chuka University College(2007)as a Constituent College of Egerton University	2004	Main Campus, Chuka	http://www.cuc.ac.ke/
10	Technical University of Kenya	Nairobi	2013	Kenya Technical Institute, Kenya Polytechnic, Kenya Polytechnic University College(2007)as a Constituent College of the University of Nairobi	1961	Main Campus, Nairobi	http://tukenya.ac.ke/
11	Technical University of Mombasa	Mombasa	2013	(MIOME), Mombasa Technical Institute[1966],Mombasa Polytechnic[1976],The Mombasa Polytechnic University College[2007]as a Constituent College of Jomo Kenyatta University of Agriculture and Technology	1940	Main Campus,Tudor. Satellite Campuses in Kwale and Lamu County	http://www.tum.ac.ke/

12	Pwani University	Kilifi	2013	Kilifi Institute of Agriculture, Pwani University College as a Constituent College of Kenyatta University	2007	Main Campus, Kilifi	http://www.pu.ac.ke/
13	Kisii University	Kisii	2013	Primary Teachers' Training College (1965), Secondary Teachers' College (1983), Egerton Campus(1994), Kisii University College(2007)as a Constituent College of Egerton University	1965	Main Campus, Kisii Town Campus	http://www.kisiiuniversity.ac.ke
14	University of Eldoret	Eldoret	2013	Chepkoilel University College as a Constituent College of Moi University		Main Campus Eldoret	http://www.uoeld.ac.ke/
15	Maaasai Mara University	Narok	2013	Narok University College as a Constituent College of Moi University	2008	Main Campus, Narok	http://www.narokuniversity.ac.ke/
16	Jaramogi Oginga Odinga University of Science and Technology	Kisumu	2013	Bondo Teachers Training College, Bondo University College, as a Constituent College of Maseno University	(2009)	Main Campus, Lake Victoria	http://www.bondo-uni.ac.ke
17	Laikipia University	Laikipia	2013	LSFTC(1965),AHITI(1979),Egerton University Campus(1990), Laikipia University College, as a Constituent College of Egerton University		Main Campus, Nyahururu town Campus, Naivasha Campus, Maralal Campus	http://laikipia.ac.ke
18	South Eastern Kenya University	Kitui	2013	Ukamba Agricultural Institute (Ukai), South Eastern University College (Seuco)	2008	SEKU Main Campus, Machakos Town Campus,Kitui Town Campus,Wote Town Campus,Mtito-Andei Campus, Mwingi Campus, Tala Campus, Nairobi City Campus.	http://www.seuco.ac.ke/
19	Multimedia University	Nairobi	2013	Central Training School. (CTS) to serve East African Posts Training	2008	(MMU) Main Campus	http://www.mmu.ac.ke/

	of Kenya			School(1948),(KCCT)Kenya College of Communications Technology (1992), Multimedia University college of Kenya				
20	University of Kabianga	Kericho	2013	The Government School, Kabianga(1925),Kabianga Teachers' Training College(1929),Kabianga Framers Training Cente(1959), Kabianga Campus of Moi University(2007), Kabianga University College	2009	(UoK)Main Campus, Kapkatet Campus, Kericho Sattellite Campus,Satellite Campus	http://www.kabianga.ac.ke/	
21	Karatina University	Karatina	2013	Moi University Central Kenya Campus, Karatina University College	2008	Main Campus,Karatina Town Campus,Itiati Campus, Nanyuki Campus, Riverbank Campus	http://www.karatinauniversity.ac.ke/	
22	Meru University of Science and Technology	Meru	2013	(MECOTECH)Meru College of Technology(1979),(MUCST)Meru University College of Science and Technology	2008	MUST Main Campus, Meru Town Campus	http://www.must.ac.ke	

Source: Wikipedia, the free encyclopedia

Appendix 1I: Questionnaire

The questionnaire is meant to get your opinion on the influence of human element on information security in your university. The questionnaire has two parts. Please respond to each item as asked. Your name is not necessary and is not required anywhere in the questionnaire. The information you provide will be treated with confidentiality.

Part A: Demographic Information

The questions below relate to your personal details, kindly tick (√) as appropriate

1. Tick(√)Your highest academic qualification

Diploma	( )
Undergraduate	( )
Masters	( )
PhD	( )
Others (specify)……..	( )

2. Kindly indicate your position in the organization? ……

Part B: Information Security

3. Which statements are true regarding your information security policy (tick all that apply)

Documented	( )
Approved by management	( )
Published	( )
Communicated to ALL employees	( )
Communicated to all third parties	( )

No information security ( )

4. What percentage of employees is aware of your information security policy? (Please tick estimated value)

   Less than 10% ( )

   Less than 30% ( )

   Less than 50% ( )

   More than 50% ( )

   More than 80% ( )

5. What percentage of employees understands their information system security responsibilities? (Tick appropriate estimate)

   Less than 10% ( )

   Less than 30% ( )

   Less than 50% ( )

   More than 50% ( )

   More than 75% ( )

6. What information is considered sensitive/critical? (Tick all that apply)

   Student information (e.g. marks) ( )

   Financial information ( )

   Communication with other universities ( )

   Expansion strategies ( )

7. What mechanisms do you use to protect data center from physical access by unauthorized persons (tick all that are applicable)

   No restriction ( )

   Entry card ( )

   A guard ( )

   Biometrics ( )

   Lock and key ( )

8. After how long do you revoke access rights for an employee who resigns or is dismissed from your university? (Please tick as appropriate)

Some days upon resignation/dismissal	( )
Immediately on receiving resignation/dismissal letter	( )
When he/she clears with the university	( )
As advised by the IT in charge	( )
No policy on revoking rights	( )

9. What is true about your back up policy? (Please tick all that is applicable)

We take daily incremental back ups.	( )
We take daily full back ups.	( )
Weekly full back ups.	( )
Monthly full back ups.	( )
Yearly full back ups.	( )

10. Does your university have constituent colleges/campuses?

Yes	( )
No	( )

11. Which technologies are used to interlink your colleges/campuses? (Please tick all that is applicable)

Digital leased lines	( )
Analogue leased lines	( )
VSAT	( )
Wireless technology	( )
GPRS/EDGE (GSM technology)	( )
Fibre Optic	( )
Colleges/Campuses not connected	( )

12. What mechanism do you use to protect your network from internet and third parties (please tick as applicable)

Access lists. ( )

Fire walls. ( )

Intrusion detection systems. ( )

Strong passwords. ( )

Access policies on all terminals. ( )

None. ( )

Not sure. ( )

13. After how long are the servers configured to lock automatically when not in use?(please tick as appropriate)

Not configured to lock out automatically. ( )

5 minutes. ( )

10 minutes. ( )

30 minutes. ( )

30 minutes. ( )

1 hour. ( )

14. After how long are the work stations configured to lock out automatically when not in use? (please tick appropriately)

Not configured to lock automatically. ( )

5 minutes. ( )

10 minutes. ( )

30 minutes. ( )

1 hour. ( )

15. How often are the employees sensitized through training on information system security (please tick appropriately).

Not sensitized ( )
Only once ( )
Regularly ( )

16. How often do you review the information security policy (please tick where applicable)

Never reviewed ( )

After 3 months ( )
After six months ( )
After one year ( )
After a security incident ( )

17. What policy do you employ to control access of information? (Please tick where applicable)

No restriction ( )
PIN number ( )
Entry card ( )
Username and password ( )
Biometrics ( )

18. What does your university's policy state about reporting information security events and weaknesses (please tick appropriately)

No policy on reporting security events ( )
Not sure ( )
Report to ICT ( )
Report to help desk ( )
Write e-mail to all staff ( )

19. Does senior management regularly receive reporting on the status of information security status or on security incidents?
Yes ( )
No ( )
20. Do you consider that senior management has an appropriate understanding of the importance of information security?
Strongly agree ( )
Agree ( )
Neutral ( )
Disagree ( )
Strongly agree ( )
21. Does senior management provide the required level of support for information security; if so in what ways has this been demonstrated?
Strongly agree ( )
Agree ( )
Neutral ( )
Disagree ( )
Strongly agree ( )

……..

22. If Senior Management involvement in security were to improve, what changes would be required, and how would these changes be reflected in specific senior management actions?

……

……

……

23. What is the operational structure for security management and who does the person with security responsibility most directly report to?

……

……

……

24. How would you describe the main approaches that are taken to manage information security?

	Yes
A structured information security management program or strategy exists	
Security is managed as part of the IT operational plan	
Security is project based	
Security is driven by risk management	
Security is driven by incident management	
Security is primarily guided by security standards	
Ad an hoc approach is applied to security	

25. Is the current management approach you have adopted proving to be an effective one in terms of achieving security requirements?
    - Strongly agree ( )
    - Agree ( )
    - Neutral ( )
    - Disagree ( )
    - Strongly agree ( )
26. What changes would be required to improve the effectiveness of your institution's information security management approach?

……

……

……

27. Do you currently use any security management standards and if so, how have standards been effective in helping with the management of information security?

……

……

……

28. Does security policy development and implementation result in the required level of involvement and support from relevant technical stakeholders?
    - Strongly agree ( )
    - Agree ( )
    - Neutral ( )
    - Disagree ( )

Strongly agree ( )

29. Does your institution treat security policies as an essential component of managing information security? (i.e. are security policies and their compliance treated seriously or taken lightly...)
    Strongly agree ( )
    Agree ( )
    Neutral ( )
    Disagree ( )
    Strongly agree ( )
30. Do you operate a structured and formal security awareness program, or is the process for security awareness more of an ad hoc one?

……

……

……

31. What types of awareness activities are undertaken, to what audience and how often?

……

……

……

32. Is raising security awareness an activity that is given an important priority?
    Yes ( )
    No ( )
33. What are the types of activities or events, or situations that have resulted in an outcome that has been very effective in raising security awareness in your institution?

……

……

……

34. Are the existing security activities that are currently undertaken adequately addressing requirements for security awareness?
    Strongly agree ( )
    Agree ( )
    Neutral ( )
    Disagree ( )
    Strongly agree ( )
35. If security awareness is below the level that it should be, what should be occurring to address this?

……

……

……

36. Is a 'culture of compliance' towards information security reflected through your institution's work practices and business processes?
    Yes ( )
    No ( )
37. Do you consider your institution to be well-positioned to 'detect and defend' against security incidents (including cyber-attacks and malicious software)?
    Yes ( )

No ( )

38. What do you consider to be the top three main causes of security incidents in your institution?

	Yes
Viruses and malicious software	
Cyber or internal based attacks	
System or software errors	
System administrator errors or non-compliance	
User errors or non-compliance	
Hardware failure	
Environmental failure	
Student riots/unrests	

39. What sort of current security issues (technology, process or people based) are you most concerned about?

……

……

……

40. What types of either new security technologies or other measures to increase compliance are you considering over the next 1 to 2 years?

……

……

……

41. What do you consider to be the top three barriers or obstacles to achieving improved security compliance in your institution?

	Yes
Funding and Resourcing	
Awareness and understanding	
'Culture of Compliance' (work practices and business processes)	
Technology Deficiencies (lack of or inadequate)	
Incident detection and response capability	
Clear Direction in Security Governance	
Organizational Commitment and Support	
Inadequate Industry Security Standards	
Capacity to measure effectiveness or value of security	
Capacity to measure effectiveness or value of security	

42. Does your university carry out information security audit?

Yes ( )

No ( )

43. What do you consider to be 'critical success factors', for the successful management of information security? (i.e. in your view, what are the key essential factors necessary for 'getting it right')?

……

……

……

Thanks a lot for your time.