# UNIVERSITY OF NAIROBI

**SCHOOL OF COMPUTING AND INFORMATICS**

# INFORMATION SECURITY MANAGEMENT SYSTEMS IN PUBLIC UNIVERSITIES IN KENYA: A GAP ANALYSIS BETWEEN COMMON PRACTICES AND INDUSTRY BEST PRACTICES

**BY**

**PHILIP MUTISYA KITHEKA**

**P56/60553/2011**

**SUPERVISOR**

**PROF. ELIJAH I. OMWENGA**

**JULY 2013**

**A research project submitted in partial fulfillment of the requirements for the award of Masters of Science Degree in Information Systems**

## DEDICATION

I lovingly dedicate this research to my family, who offered me unconditional love and support throughout the course of this research.

## DECLARATION

I certify that this research project entitled "Information security management systems in public universities in Kenya: A gap analysis between common practices and industry best practices" is my own work. The work has not been presented elsewhere for assessment. Where material has been used from other sources it has been properly acknowledged.

**SIGNED** _____ **DATE** _____

**Philip Mutisya Kitheka**
**Registration No. P56/60553/2011**

I certify that this project has been submitted for examination with my approval as the University of Nairobi supervisor.

**SIGNED** _____ **DATE** _____

**Prof. Elijah I. Omwenga**
**School of Computing and Informatics**
**University of Nairobi**

## ABSTRACT

This research is concerned with issues regarding information security management in public universities in Kenya motivated by the need for implementing effective information security management systems. Universities in Kenya are increasingly using information technology (IT) for essential business operations including administration, teaching, learning and research. These technology assisted initiatives however depend on availability of enabling infrastructure and ultimately on how well that infrastructure is secured and protected.

The main aim of this research was to investigate current information security management practices in Kenyan public universities. To help information security practitioners in these institutions to implement effective information security management systems, a framework for information security management grounded on industry best practice guidelines and recommendations in information security management was proposed. The framework guided a comprehensive study to understand the information security control environment in public universities in Kenya.

A descriptive survey targeting information security professionals and users of information systems was carried out in five public universities selected randomly. In total, 31 respondents participated in this survey representing a response rate of 58.5%. Descriptive statistics was used for data analysis. Additionally, binomial tests using SPSS were used to evaluate the relationship between dependent variable and the independent variables. Main data collection instrument was a questionnaire.

The study findings indicate that the information security control environment in public universities is inadequate to deal effectively with information security threats. The main barriers to information security include enforcement of policies, lack of senior management support and lack of resources. This study has made tremendous contributions to the domain of information security management. Information security practitioners in public universities attempting to implement information security management systems can use the proposed framework to benchmark their ISM practices. Furthermore, the main issues, barriers and factors that influence information security management have been highlighted with recommendations about how to address them to secure information assets.

## ACKNOWLEDGEMENTS

I would like to express my deep appreciation to my supervisor Professor Elijah I. Omwenga for his support, guidance and encouragement during the entire period of this research. Special thanks to Mr Joseph Ogutu, Dr. Robert Oboko and Dr Agnes Wausi for their support and recommendations, which helped improve this thesis.

I would also like to thank all Lecturers, Directors, IT professionals and all other individuals in the various public universities who participated in this research, for their help and co-operation; without them I would not have been able to complete my research. Due to confidentiality, I cannot mention their names.

Last but not certainly not least, I am forever indebted to my wife Phyllis Mwende and my sons Emmanuel, Joseph and James for their endless patience and support.

Thank you all.

**Philip Mutisya Kitheka**
**Registration No. P56/60553/2011**

# TABLE OF CONTENTS

## LIST OF TABLES

## LIST OF FIGURES

## ACRONYMS

IT – Information Technology

ICT-Information and communications technology

ISMS – Information security management system

ISM – Information security management

CN – Contingency planning

DRP – Disaster recovery plan

IRP – Incident response plan

BIA – Business impact analysis

CIA – Confidentiality, integrity and availability

TEAMS -The East African Marine System the East African

EASSy - Submarine Cable System

LION2 - Lower Indian Ocean Network (LION2)

NIST - National Institute of Standards and Technology

COBIT - Control Objectives for Information and related Technology

ITIL - The Information Technology Infrastructure Library

# CHAPTER ONE

# INTRODUCTION

## 1.1 Background

Universities in Kenya are increasingly using information technology (IT) for essential business operations including administration, teaching, learning and research. As an example, a great number of public universities in Kenya are using technology-enhanced learning (e-learning) to remove geographical and financial barriers to higher education (Ministry of Higher Education, 2007). Using different platforms, students are able follow lectures online, interact with lecturers, submit assignments and check on their grades. Lecturers are also able to upload course materials, post assignments and generate discussions online using blogs. These technology assisted initiatives however depend on availability of enabling infrastructure and ultimately on how well that infrastructure is secured and protected. It is thus very crucial for information security practitioners in these institutions to implement truly effective information security programs. This can be achieved by implementing internationally recognized best practice recommendations and guidelines on information security management(ISM).

In the area of information security, various standards and guidelines have been developed and published that can help to establish, implement, operate, monitor and maintain effective ISMS. Some of these standards and guidelines include ISO/IEC 27001 (the international replacement for BS7799-2:2002), ISO/IEC 27002 (which was, until recently, known as ISO/IEC 17799) and National Institute of Standards and Technology (NIST) 800 special publications (Arnason and Willet, 2008). ISO 27001 and ISO 27002 are security standards focusing mainly on information security. An organization may choose to use the ISO 27001 and 27002 standards as the basis for implementing and maintaining a good information security management system (Calder and Watkins, 2008). These standards are however generic and therefore have to selectively applied depending the kind of institution.

This thesis is concerned with issues relating to the management of information security in public universities in Kenya, motivated by the need for implementing effective information security management systems. Furthermore, the study is motivated by the relative lack of an appropriate framework for information security management in public universities in Kenya.

By definition, Information security management system refers to set of coordinated activities to direct and control the preservation of confidentiality, integrity, and availability of information (Tipton and Krause, 2000). According to Calder and Watkins (2008), "Information security management systems in the vast majority of organizations are, in real terms, non-existent, and even where systems have been designed and implemented, they are usually inadequate". This means that most organizations are vulnerable to a wide range of possible threats whose origin may be internal or external to the organization. According to a study by Deloitte East Africa (2011), insiders present a bigger security threat to organizations in east Africa than outsiders.

Today, institutions of higher learning are producing more data than ever before. This data is being shared faster and more widely than in the past. Additionally, Attacks upon information security infrastructures have continued to evolve steadily overtime making the management of information security more complex and challenging than ever before (Deloitte East Africa, 2011). Legacy network based attacks have largely been replaced by more sophisticated web application based attacks. According to Educause Center for Applied Research (2003), Successful security efforts require not only increased investment in technologies, personnel, and software but also training and user education on information security threats.

### 1.1.1 Trends in information security breaches in Kenya

News headlines in recent months have demonstrated the importance of organizations to adopt an effective approach to Information Security Management (ISM) by illustrating what can happen in its absence. In one of the most widely publicized incidents, one hundred and three (103) government websites hosted on the dot go.ke domain were hacked overnight by an Indonesian cyber-security student (CIO East Africa, 2012). The hacker claimed that he took down the websites following tutorials from an online Indonesian security forum known as Forum Code Security. It is very unlikely that information technology security controls were not in place to prevent these incidents but the attacks were successful.

Similar incidents have also been witnessed in public and private universities in Kenya. A recent report circulated to all Vice Chancellors of public universities and Principals of University Colleges dated 24$^{th}$ October 2011 from the Office of the Permanent Secretary, Ministry of Higher Education, Science and Technology contained information that a third year computer

science student of Catholic University of Eastern Africa (CUEA) in conjunction with other students in the faculty had been hacking in computer systems of various universities altering grades and clearing fees balances. This report further stated that the most affected institutions were the Catholic University of Eastern Africa, Daystar University, Maseno University and the Jomo Kenyatta University of agriculture and Technology (JKUAT).

In yet another incident, on December 6th 2011, a syndicate of employees and students of Kenyatta University hacked into the institution's online database and altered examination results (The Star, 2011). Due to the alterations, the university struck off names of many students who were scheduled to graduate on December 9th 2011. As a result, a student by the name Alice Njeri filed a case in court accusing the University of striking off her name unfairly from the graduation list.

These are just the few incidents of information security breaches in public and private universities in Kenya that have made headlines, others have never been reported for the simple reason that, the affected institutions fear that their image and reputation would be at stake. These incidents demonstrate the ineffectiveness of information security management systems currently in use or even worse, the non-existence of information security programs in some of the institutions. Best practices in information security call for the need to ensure information security management systems are implemented, maintained, monitored and reviewed regularly to ensure their effectiveness (Arnason and Willet, 2008). Information security controls should be selected, implemented and tested for their effectiveness as part of a comprehensive information security management program.

### 1.1.2 Challenges of information security management in public Universities in Kenya

Information security management in universities is challenging and complex. Since Universities are havens of free exchange of knowledge and ideas, they must uphold the principles of academic freedom and the free exchange of ideas and therefore information security policies and programs are expected to support those principles while still maintaining an appropriate level of security (Educause Center for Applied Research, 2003). As such, it would be impossible to completely lockdown staff and student Personal computers and thus the greatest challenge is to ensure that information systems are open and flexible, yet as secure as possible. Additionally,

those who are looking to steal that data are becoming more sophisticated and stealthy than ever before.

The threat landscape is also evolving at a very fast rate. Many students and employees alike use social networking sites like facebook and tweeter to exchange information about themselves, share pictures and videos, and use blogs and private messaging to communicate with friends. Institutions of higher learning have also benefited from cheaper bandwidth courtesy of The East African Marine System (TEAMS) fiber optic cable project, Seacom, the East African Submarine Cable System (EASSy) and Lower Indian Ocean Network (LION2), all which provide direct access to worldwide international cable networks. Furthermore, a variety of devices, such as desktop and laptop computers, Personal Digital Assistants (PDAs) and mobile/cellular phones, each with the capability to access information located at institution's data centers are typically being used. This opens the attack space and unless a properly designed and adequate information security strategy is adopted, incidents of information security breaches shall continue to occur.

While most institutions believe that their information systems are secure, the reality is that they are not (Calder and Watkins, 2008). These institutions often inaccurately perceive information security as the state or condition of controls at a particular point in time. Security is an ongoing process, whereby the condition of an institution's controls is just one indicator of its overall information security posture. Other indicators include the ability of the institution to continually assess its information security posture and react appropriately in the face of rapidly changing threats, technologies, and business conditions.

According to Deloitte East Africa (2011), most organizations in East Africa are ill prepared to deal with information security threats. In this study, Deloitte East Africa (2011) have stated that while most organizations have established security programs and plans, this alone doesn't guarantee protection from all security breaches. The study further suggests that organizations should not only emphasize preventing risks but also enabling effective response capabilities.

## 1.2 The Research Problem

One of the greatest challenges facing universities in Kenya today is how to effectively manage the security of information systems that support teaching, learning and research activities. Although many studies have been carried out in the area of information security in public

universities in Kenya, there is lack of a structured approach/ framework for the effective management of information security in these institutions.

A number of information security incidents have been witnessed in public and private universities in Kenya in the recent past as demonstrated in the foregoing discussion. Many of these incidents are rarely reported or even documented. Whenever Incidents involving loss of confidentiality, integrity or availability of information occur, they can be costly. Serious incidents can also be damaging to the reputation of the Universities and therefore there is need for these institutions to implement effective information security management programs and to frequently monitor, review, maintain and improve them to safeguard information technology assets. One way of achieving this is to implement information security best practice recommendations and guidelines.

The main aim of this research is to identify factors that impact of the overall effectiveness of an information security management system and to investigate information security management systems in the public universities in Kenya to determine and analyze the gaps between actual information security controls implemented and industry best practices. Furthermore, a conceptual framework for effective management of information security in public universities in Kenya is proposed. This framework can be used by information security practitioners attempting to implement information security programs to benchmark their processes and practices.

### 1.3 Research objectives

The specific objectives of this research are:

(i) To determine key factors that influence the overall effectiveness of an information security management system

(ii) Develop an appropriate framework for effective information security management in public universities in Kenya.

(iii) To investigate information security management practices in Kenyan public universities.

(iv) To determine and analyze the gaps between information security management practices in public universities in Kenya and internationally recognized best practice recommendations and guidelines in information security management.

## 1.4 Research question(s)

This research is designed to answer the following research question.

(i) What factors determine the overall effectiveness of an information security management system?

(ii) Is there an existing framework for information security management in Kenyan public universities?

(iii) Are information security professionals in public universities in Kenya adhering to best practices in information management?

(iv) What gaps exist between common information security management practices and industry best practices?

## 1.5 Significance of the study

Research focusing specifically on information security management in Kenyan public universities has received little academic focus. This is despite growing dependency on information technology (IT) and the information systems that are developed from that technology to successfully carry out their missions and business Functions.

The study sought to understand the information security control environment in Kenyan public universities. The associated difficulties in the university environment with managing information security are key aspects of this study.

Furthermore, by identifying and analyzing the gaps that exist between information security management practices in public universities in Kenya and industry best practices and more importantly by proposing a framework for effective information security management, this research will enable information security professionals to:

(a) Rethink and review their security strategies in order to ensure security of their technology assets.

(b) Benchmark their ISM practices to ensure adequate protection of information assets

(c) Incorporate measures necessary to implement reliable and secure information technology infrastructure necessary for technology enabled learning and academic research.

## 1.6 Definition of terms

**Threats:** Actions or events that potentially compromise the confidentiality, integrity, availability, or authorized use. These threats may be human or non-human, natural, accidental, or deliberate.

**Vulnerability:** Vulnerability is a weakness in an information system or its components that could be exploited.

**Asset:** Asset is anything that has value to the organization. . The asset could be the computer system or the data it holds.

**Information security:** Preservation of confidentiality, integrity, and availability of information.

**Information security Management system (ISMS):** Information security management system refers to set of coordinated activities to direct and control the preservation of confidentiality, integrity, and availability of information

**Cryptography:** the principles, means, and methods for rendering information unintelligible and for restoring encrypted information to intelligible form.

**Risk**: A combination of the likelihood that a threat will occur, the likelihood that a threat occurrence will result in an adverse impact, and the severity of the resulting adverse impact

**Risk analysis**: A formal systematic approach to assessing the vulnerability of an information technology system or installation. Risk analysis is the process of analyzing threats to and vulnerabilities of an information system to determine the risks (potential for losses).

**Risk Management:** Risk management is a coordinated set of activities to identify and assess security vulnerabilities and put in place countermeasures (controls) to reduce the residual risk to the level agreed in the security policy which has been designed to meet the organization's business needs.

**Authentication:** The process of verifying that users are who they claim to be when logging onto a system. Generally, the use of user names and passwords accomplishes this. More sophisticated is the use of smart cards and retina scanning. The process of authentication does not grant the user access rights to resources - this is achieved through the authorization process.

**Authorization:** The process of allowing only authorized users access to sensitive information. An authorization process uses the appropriate security authority to determine whether a user should have access to resources.

**Information Technology (IT) Contingency Planning:** information technology contingency planning refers to the dynamic development of a coordinated recovery strategy for information systems (major application or general support system), operations, and data after a disruption ( NIST, 2002).

**Disaster Recovery Planning:** The advance planning and preparations necessary to minimize loss and ensure continuity of the critical business functions of an organization in the event of disaster. A Disaster Recovery Plan (DRP) is the document that defines the resources, actions, tasks and data required to manage the business recovery process in the event of a business interruption.

**Business Impact Analysis:** This is the process of analyzing all business functions and the effect that a specific disaster may have upon them. The business impact analysis (BIA) is used to identify and prioritize the components of an system by correlating them to the business processes the system supports, and by using this information to characterize the impact on the processes if the system were unavailable.

# CHAPTER TWO

# LITERATURE REVIEW

## 2.1 Introduction

The proliferation of increasingly complex, sophisticated and global threats to information security is driving organizations of all kinds to take a more strategic view of information security (Calder and Watkins, 2008). To address the situation, many different information security standards and guidelines have been proposed and developed. A number of governments and organizations have developed standard bodies whose function is to setup benchmarks, standards and in some cases legal regulations on information security to help ensure an adequate level of security is maintained, resources are used appropriately and the best security practices are adopted.

## 2.2 Information Security Management Systems

Information security management system refers to set of coordinated activities to direct and control the preservation of confidentiality, integrity, and availability of information (Tipton and Krause, 2000). An information security management system (ISMS) is necessary because the threats to the availability, integrity and confidentiality of the organization's information are great, and always increasing (Calder and Watkins, 2008).

## 2.3 Key Information Security Management Concepts

The overall objective of an information security program is to protect the confidentiality, integrity and availability of an institution's information (Peltier et al., 2005).

**Confidentiality:** Assurance that information is shared only among authorized persons or organizations. Breaches of Confidentiality can occur when data is not handled in a manner adequate to safeguard the confidentiality of the information concerned. Such disclosure can take place by word of mouth, by printing, copying, e-mailing or creating documents and other data.

**Integrity:** Assurance that the information is authentic and complete. The term Integrity is used frequently when considering Information Security as it represents one of the primary indicators of security (or lack of it). The integrity of data is not only whether the data is 'correct', but also whether it can be trusted and relied upon.

**Availability:** Assurance that the systems responsible for delivering, storing and processing information are accessible when needed, by those who need them.

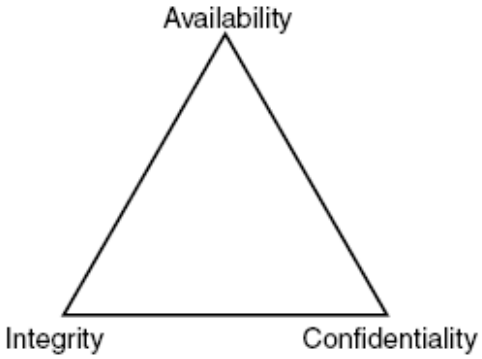


**Figure 1: CIA Triad**

***Source: Peltier et al. (2005, p. 39)***

## 2.4 Defense in depth security strategy

The principle of defense-in-depth is that layered security mechanisms increase security of the system as a whole. If an attack causes one security mechanism to fail, other mechanisms may still provide the necessary security to protect the system (Tipton and Krause, 2000). By implementing enough layers of protection the likelihood of compromise is drastically reduced.

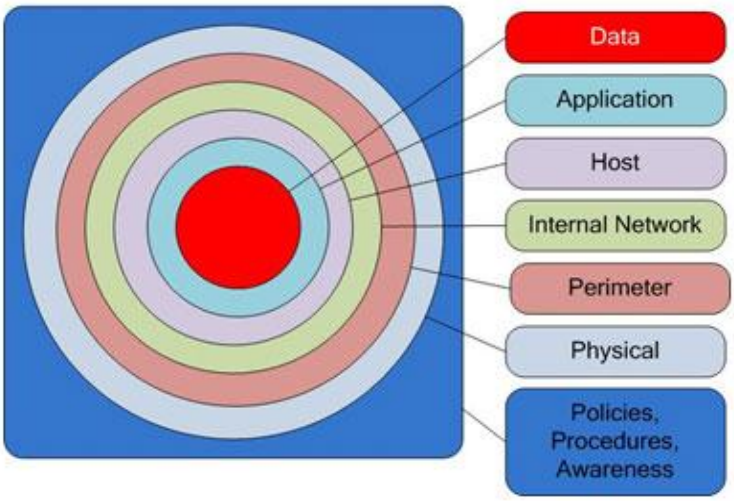


**Figure 2: Defense in depth layers**
**Source: http://technet.microsoft.com/en-us/library/cc512681.aspx**

### 2.4.1 Defense in depth layer one: Policies, procedures and awareness

Security policies should be the foundation of every Defense in Depth plan. Policies promote best practices and the protection of information assets. The overall effectiveness of policies however depends on how well they are communicated, promoted and enforced. Procedures spell out the step-by-step specifics of how the policy and the supporting standards and guidelines will actually be implemented in an operating environment. Users should also be aware of the need for information security and its significance. They should also understand security related processes and procedures as well as the consequences of a security breach.

### 2.4.2 Defense in depth Layer two: Physical security

Physical security is primarily concerned with restricting physical access by unauthorized people to facilities hosting information technology assets. Security components in this layer include closed-circuit television cameras (CCTV), locks and burglar alarms.

### 2.4.3 Defense in depth Layer three: Perimeter security

The perimeter security layer, refers to the point at which traffic passes from the outside (untrusted) network to the inside (trusted) network. Network Firewall is the most obvious consideration but there are other important network security components. The firewall allows or denies access to and from different attached network segments based on the ruleset applied. Various other types of protection can also be deployed in this layer, including malware protection, spam filtering, content filtering and intrusion detection and prevention.

### 2.4.4 Defense in depth Layer four: Internal Network

The focus in this defense in depth layers is protection of the corporate IT infrastructure. The network and associated communications infrastructure also offers an opportunity to provide the greatest security coverage of information within an organization. Common controls in this defense in depth layer include:

- A suitable authentication technique (knowledge, token, biometric based) should be chosen to authenticate the users.
- Network intrusion detection as a means of monitoring and identifying malicious activity throughout the network and Network intrusion prevention to prevent external exploits from reaching the internal network where they may be actualised.

- Network segregation through routers, switches, firewalls and other devices.
- Traffic encryption to prevent eavesdropping of sensitive data being transported across the network and internet.
- Centralised authentication to keep unauthorised users from accessing the corporate network
- Content filtering to prevent malicious software from entering the network.

### 2.4.5 Defense in depth Layer five: Host

All network traffic has a source and a destination device. Destination devices include workstations, servers, phones and other mobile devices. Anti-virus software is a critical component of host layer security, and security personnel should ensure that the software is installed on every server and workstation and is regularly updated. Other considerations include:

- Patch management
- Making sure only necessary services are running
- Application control
- Host intrusion detection and prevention
- Host based firewall
- Strong file permissions

### 2.4.6 Defense in depth Layer six: Application

Software applications are also targets of attack. These applications include payroll, database applications and other varieties of applications typically found in most organizations. Comprehensive protections at the application security layer include access controls to authenticate, authorize and account for secure communications to an application or service. Code protection is also necessary. Routine software maintenance is an important consideration to ensure all patches related to security flaws are current. Security concerns should also be addressed during the design and implementation of applications. Other considerations include strong authentication using proven cryptographic techniques and where possible multiple ‘factors’.

### 2.4.7 Defense in depth Layer seven: Data

The final layer in a defense-in-depth security policy protects the sensitive data itself. Protection strategies at this layer focus on stored data and also information in transit. Encryption is a key component in this layer.

## 2.5 The role of standards

Information security standards can provide the basis to safeguard information assets. In the area of information security, various standards and guidelines have been developed and published that can help to address the requirements of an information security management system. These standards however are often general guidelines or principles that may not all be applicable to a particular organization.

## 2.6 Overview of information security management standards and frameworks

Various standards and best practice frameworks exist to help organizations assess their security risks, implement appropriate security controls, and comply with governance requirements as well as privacy and information security regulations. They include ISO 27001, ISO 27002, ITIL, COBIT and NIST 800 series. Although no single industry security standard provides all the answers to information security needs, a good industry standard does provide a widely accepted, proven framework within which to define a security program and it provides a foundation from which to build that security program to satisfy the particular needs of a particular organization (Arnason et al., 2008).

### 2.6.1 ISO 27001

The ISO 27001 international standard formally defines the mandatory requirements for an Information Security Management System (ISMS). It is the international Code of Best Practice for Information Security from the International Standards Organization in Geneva. The standard promotes the adoption of a process approach for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an organization's information security management system (ISMS).

This international standard is designed to ensure the selection of adequate and proportionate security controls to protect information assets. This standard is usually applicable to all types of

organizations, either private or public organizations. The standard adopts the "Plan- Do-Check-Act" (PDCA) process model, which is applied to structure all ISMS processes (Calder and Watkins, 2008).

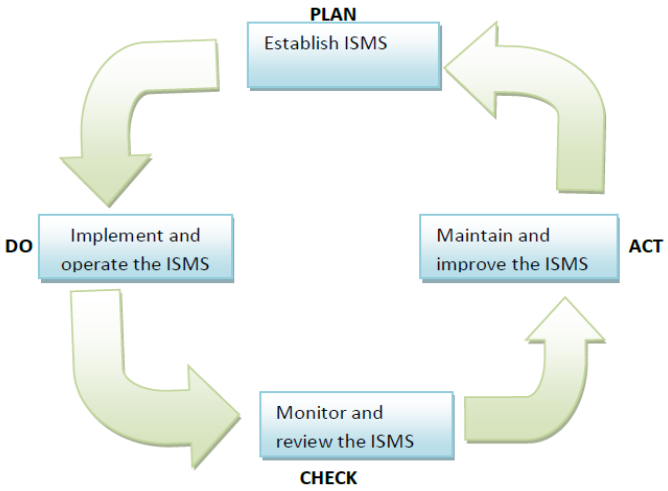


**Figure 3: PDCA Model applied to ISMS Processes**
***Source: Arnason and Willet (2008, p.7)***

### 2.6.2 ISO 27002

ISO 27002, *Code of Practice for Information Security management*, is a commonly used international standard for information security throughout the world and provides insight to security controls to protect information and information technology. This standard contains guidelines and best practices recommendations for 10 security domains:

- Security policy
- Organization of information security
- Asset management
- Human resources security
- Physical and environmental security
- Communications and operations management
- Access control
- Information systems acquisition, development and maintenance
- Information security incident management
- Business continuity management
- Compliance

### 2.6.3 COBIT

The ‘Control Objectives for Information and related Technology’ is a set of best practices for IT governance created by the Information Systems Audit and Control Association (ISACA), and the IT Governance Institute (ITGI) in 1992. COBIT is increasingly internationally accepted as good practice for control over information, IT and their related risks (Information Systems Audit and Control Association).

The COBIT framework contains 34 key information technology processes in four domains (Planning and Organization, Acquisition and Implementation, Delivery and Support & Monitor and Evaluate). These IT processes provide a basis for establishing and maintaining good security.

Of particular relevance to the implementation of the principles of information security, these COBIT IT practices can be used to define the information security tasks.

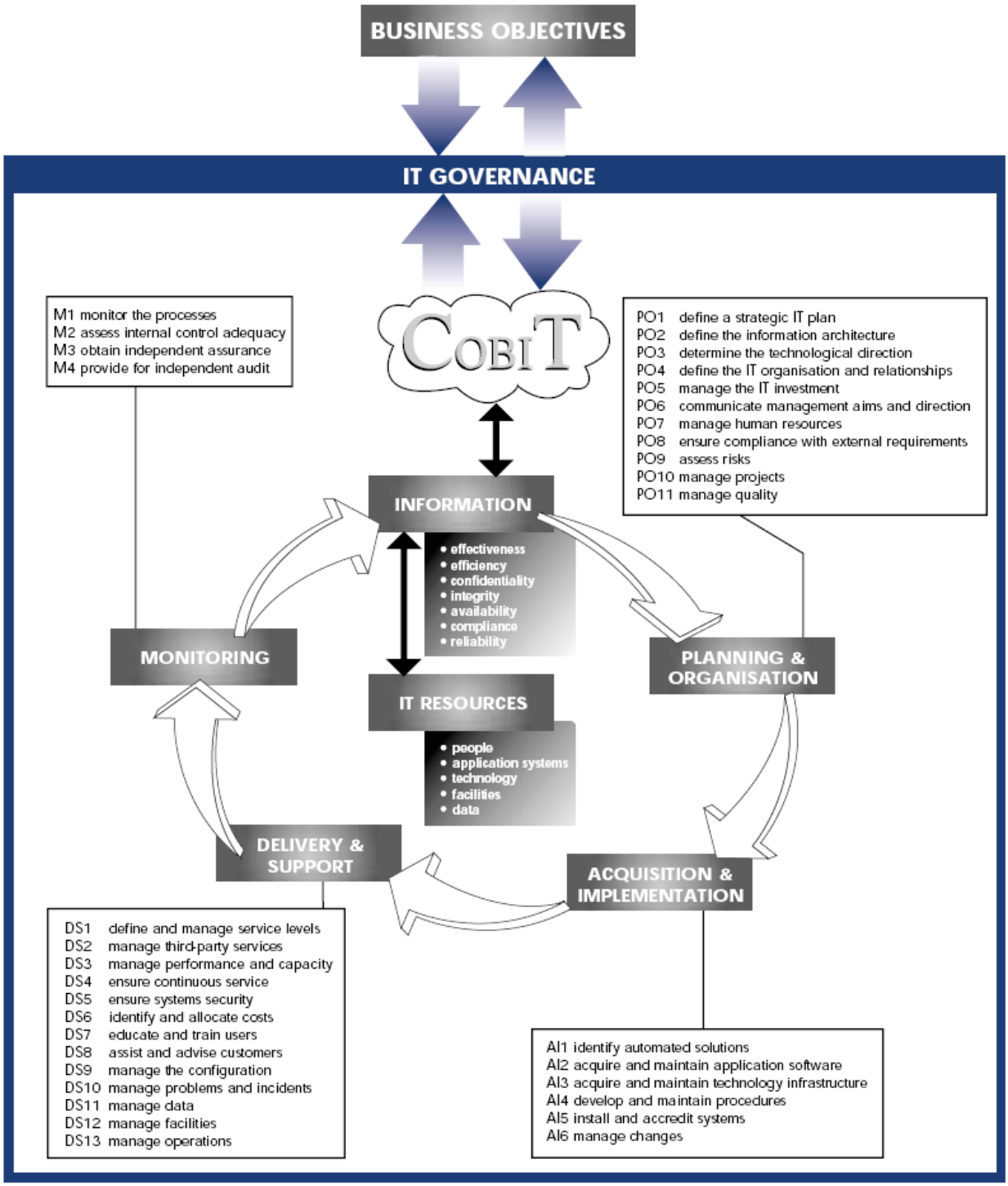


**Figure 4: The COBIT Framework**

***Source: Information Systems Audit and Control Association (ISACA)***

### 2.6.4 National Institute of Standards and Technology (NIST) Special Publications – NIST 800 series

The NIST 800 Series is a set of documents that describe United States federal government computer security policies, procedures and guidelines. Special Publications in the 800 series present documents of general interest to the computer security community. The Special Publication 800 series was established in 1990 to provide a separate identity for information technology security publications.

### 2.6.5 ITIL

The Information Technology Infrastructure Library (ITIL) is a best practice IT Service Management process framework developed by the Office of Government Commerce (OGC) within the UK government. ITIL is the most widely accepted approach to IT service management in the world.

A component of ITIL, ITIL Security Management based on ISO 17799 is of particular relevance to the application of the information security principles. The ITIL Security Management component is procedure based and includes ITIL standard processes such as service level, incident and change management processes.

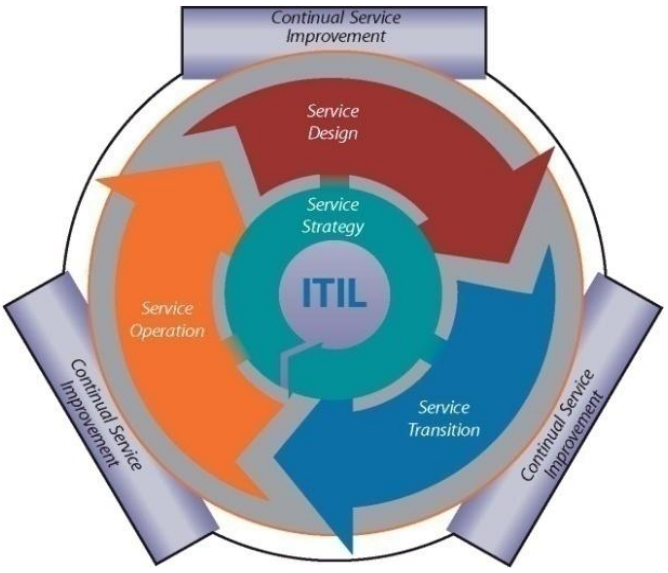


**Figure 5: The Components of ITIL V3**

***Source: Sante and Ermers (2009)***

### 2.6.6 PCIDSS

The Payment Card Industry Data Security Standard (PCIDSS) is a worldwide information security standard defined by the Payment Card Industry Security Standards Council to enhance payment account data security. The standard was created to help organizations to securely process card payments and to prevent credit card fraud through increased controls. The standard applies to all organizations that hold, process, or exchange cardholder information from any card branded with the logo of one of the card brands.

## 2.7 Information security management best practices

All organizations possess information, or data, that is either critical or sensitive (Calder and Watkins, 2008). Given this, the priority attached to information security should remain high. It is therefore very important that organizations take appropriate steps to secure and protect their information assets. Best practices for information security as provided for in various information security guidelines, standards and frameworks can be used to help secure information technology (IT) systems and networks.

### 2.7.1 Security Policy

According to Peltier et al. (2005), the cornerstone of effective information security architecture is a well written security policy. A security policy is a formal statement of the rules by which people who are given access to an organization's technology and information assets must abide. Because a policy is typically written at a broad level, organizations must also develop standards, guidelines, and procedures that provide employees with a clear approach to implementing the policy (NIST, 2003).

In order for a security policy to be appropriate and effective, it needs to have the acceptance and support of all levels of employees within the organization. The ISO 27001 standard requires that the security policy document (A.5) should be approved by management, published and communicated as appropriate to all employees (Calder and Watkins, 2008). It should state management commitment and set out the organization’s approach to managing information security.

### 2.7.2 Organization of information security

In control A.6 of the ISO 27001 standard, Management is required to actively support security within the organization through clear direction, demonstrated commitment, explicit assignment, and acknowledgement of information security responsibilities. Information security activities should be co-ordinated by representatives from different parts of the organization with relevant roles and job function. In addition, confidentiality agreements or non-disclosure agreements reflecting the organization's needs for the protection of information should be identified and regularly reviewed (ISO27k Forum, 2011).

### 2.7.3 Information Security Awareness and training

Information security awareness and training is another very important aspect of a good information security program. According to Arnason and Willet (2008, pp. 109), "All employees must be aware of security issues and the need for security". Security roles and responsibilities clearly stated in the terms and conditions of employment. An institution should also perform employee orientation for information and information technology security in addition to putting in place a formal disciplinary procedure for employees who have committed a security breach (Calder and Watkins, 2008).

### 2.7.4 Risk Assessment

Risk assessment is a key part of an effective information security management system. National Institute of Standards and Technology (1995), in the special publication 800-12, argues that to minimize information security threats, risk identification, analysis and mitigation is paramount. This argument is also supported by Arnason and Willet (2008). Once security risks have been identified and decisions for the treatment of risks have been made, appropriate controls should be selected and implemented to ensure risks are reduced to an acceptable level.

### 2.7.5 Asset Management

Control A.7.1.1 of the ISO 27001 standard requires an organization to identify all important information assets (computer and communications hardware/systems, application software, data, and printed information) and to draw up and maintain an inventory of them. The inventory should be fully up-to-date, accurate and complete. In addition, Owners of information assets should be identified for all major assets and the responsibility for the maintenance of appropriate

controls should be assigned (ISO27k Forum, 2011). Responsibility for implementing controls may be delegated. Accountability should remain with the nominated owner of the asset (ISO27k Forum, 2011).

### 2.7.6 Physical and environmental security

Clause A.9 of the ISO27001 standard deals with physical and environmental security (ISO27k Forum, 2011). Critical or sensitive business information processing facilities should be housed in secure areas, protected by a defined security perimeter, with appropriate security barriers and entry controls. They should be physically protected from unauthorized access, damage and interference. The protection provided should be commensurate with the identified risks. Physical protection against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster should be designed and applied in addition to ensuring that access points such as delivery and loading areas and other points where unauthorized persons may enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access (ISO27k Forum, 2011). Power and telecommunications cabling carrying data or supporting information services should be protected from interception or damage (ISO27k Forum, 2011). All items of equipment containing storage media should be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal (ISO27k Forum, 2011).

### 2.7.7 Incident Reporting and Management

Information security breaches are difficult to predict and therefore an institution is in a better position to deal with information security incidents if it has implemented information security incident reporting and management procedures (NIST, 2003). This ensures that information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken. An incident-handling capability can provide the ability to react quickly and efficiently to disruptions of services.

In addition, organizations should have mechanisms in place to enable the types, volumes, and costs of information security incidents to be quantified and monitored (Calder and Watkins, 2008). Where a follow-up action against a person or organization after an information security incident involves legal action (either civil or criminal), evidence should be collected, retained,

and presented to conform to the rules for evidence laid down in the relevant jurisdictions (Calder and Watkins, 2008).

### 2.7.8 Information systems acquisition, development and maintenance

According to the ISO 27001 international standard clause A.12, Information systems should be developed, acquired, and maintained with appropriate security controls. The standard requires organizations to ensure that;

- Information systems are developed and implemented with appropriate security features enabled.
- Software is trustworthy by implementing appropriate controls in the development process, reviewing source code, reviewing the history and reputation of vendors and third party developers, and implementing appropriate controls outside of the software to mitigate the unacceptable risks from any deficiencies.
- A policy on the use of cryptographic controls for protection of information is developed and implemented.
- Implementation of changes should be controlled by the use of formal change control procedures (Calder and Watkins, 2008).
- When operating systems are changed, business critical applications should be reviewed and tested to ensure there is no adverse impact on organizational operations or security.
- Timely information about technical vulnerabilities of information systems being used should be obtained, the organization's exposure to such vulnerabilities evaluated, and appropriate measures taken to address the associated risk.

### 2.7.9 Human resources security

Control A.8 of the standard requires security responsibilities to be addressed at the recruitment stage, in contracts and during an individual’s employment. Prior to employment, organizations should ensure that employees, contractors and third party users understand their responsibilities, and are suitable for the roles they are considered for to reduce the risk of theft, fraud or misuse of facilities (Arnason and Willet, 2008). Recruits should be adequately screened, especially for sensitive jobs. During employment, Organizations should ensure that all employees, contractors and third party users are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support organizational security policy in the course of their

normal work, and to reduce the risk of human error (Arnason and Willet, 2008). All employees and third party users of information processing facilities should sign a confidentiality (nondisclosure) agreement (ISO27k Forum, 2011). Employees, contractors and third party users who leave an organization or change employment should return all of the organization's assets in their possession and their access rights to information assets removed (ISO27k Forum, 2011). In addition, there should be a formal disciplinary process for employees who have committed a security breach. All employees of the organization, contractors and third-party users, should receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant for their job function (ISO27k Forum, 2011).

### 2.7.10 Access control

Access control is the ability to permit or deny the use of a particular resource by a particular entity. In information security, access control includes authentication, authorization and audit. It also includes measures such as physical devices, including biometric scans and metal locks, hidden paths, digital signatures, encryption, social barriers, and monitoring by humans and automated systems.

Clause A.11 of the ISO27001 standard deals with access control. Access to information, and business processes should be controlled on the basis of business and security requirements. An access control policy should be established, documented, and reviewed based on business and security requirements for access. There should be procedures for user registration, user password management, review of access rights and privilege management (Calder and Watkins, 2008). In addition, Access to operating systems should be controlled by a secure log-on procedure and all users should have a unique identifier (user ID) for their personal use only, and a suitable authentication technique should be chosen to substantiate the claimed identity of a user. Sensitive systems should have a dedicated (isolated) computing environment. A formal policy should be in place, and security measures should be adopted to protect against the risks of using mobile computing and communication facilities (Calder and Watkins, 2008). Physical and logical access to diagnostic and configuration ports shall be controlled. A policy, operational plans and procedures should be developed and implemented for teleworking activities.

### 2.7.11 Communications and operations management

Responsibilities and procedures of the management and operation of all information processing facilities should be established (Calder and Watkins, 2008). Changes to information processing facilities and systems should also be controlled. Duties and areas of responsibility should be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets (Calder and Watkins, 2008).

Detection, prevention, and recovery controls to protect against malicious code and appropriate user awareness procedures should be implemented (Calder and Watkins, 2008). Back-up copies of information and software should be taken and tested regularly in accordance with the agreed backup policy. Networks should also be adequately managed and controlled, in order to be protect them from threats and to maintain security for the systems and applications using the network, including information in transit (Calder and Watkins, 2008).

According to ISO 27001 standard, there should be procedures in place for the management of removable media. Media should be controlled and physically protected. Appropriate operating procedures should be established to protect documents, computer media (such as tapes, disks, cassettes, etc) and system documentation from damage, theft and unauthorized access. Media should also be disposed of securely and safely when no longer required, using formal procedures.

Information involved in electronic messaging should be appropriately protected (Calder and Watkins, 2008). Audit logs recording user activities, exceptions, and information security events should be produced and kept for an agreed period to assist in future investigations and access control monitoring.

### 2.7.12 Business Continuity Management

As an important security measure, plans must also be in place to preserve business in the wake of a disaster or disruption of service (Stewart et al., 2008). This is called contingency planning. Contingency plans should be developed and implemented to ensure that business processes can be restored within the required time-scales (Calder and Watkins, 2008).

In clause A.14 of the ISO 27001 standard, organizations are required to implement a business continuity management process to reduce the disruption of services caused by disasters and security failures (which may be the result of, for example, natural disasters, accidents, equipment failures, and deliberate actions) to an acceptable level through a combination of preventative and recovery controls. Business continuity management should include controls to identify and reduce risks, limit the consequences of damaging incidents and ensure the timely resumption of essential operations. Business continuity plans should be tested and updated regularly to ensure that they are up to date and effective (Calder and Watkins, 2008).

### 2.7.13 Compliance

The design, operation, use and management of information systems may be subject to statutory, regulatory and contractual security requirements and therefore Appropriate procedures should be implemented to ensure compliance with legislative, regulatory and contractual requirements on the use of material in respect of which there may be intellectual property rights and on the use of proprietary software products (Calder and Watkins, 2008). Important records should be protected from loss, destruction and falsification, in accordance with statutory, regulatory, contractual, and business requirements. Cryptographic controls shall be used in compliance with all relevant agreements, laws, and regulations (Calder and Watkins, 2008). Managers should ensure that all security procedures within their area of responsibility are carried out correctly to achieve compliance with security policies and standards (Calder and Watkins, 2008).

## 2.8 Information Security threats

A good understanding of information security threats is important in the design and implementation of an effective information security management system. A threat is any circumstance or event that can potentially harm an information system by destroying it, disclosing the information stored on the system, adversely modifying data, or making the system unavailable (United States Department of Agriculture, 2011).

A Vulnerability is a weakness in an information system or its components that could be exploited (USDA, 2011).Vulnerabilities exist when there is a flaw or weakness in hardware or software that could be exploited by hackers.

Information processing systems are vulnerable to many threats that can inflict various types of damage that can result in significant losses (Peltier, T.R., Peltier J., and Blackley J., 2005). According to Deloitte East Africa (2011), insiders present a bigger security threat compared to outsiders for East African Organizations.

According to Calder and Watkins (2008), Information security threats come from both within and without an organization. According to NIST, (1995), Information security threats can be classified in to one of the following categories.

**(a) Environmental Threats:** This category of information security threats includes lightning, fires, hurricanes, tornadoes and floods. Poor building wiring or insufficient cooling for the systems can also cause harm to information systems.

**(b) Errors and Omissions:** This is the number-one threat to information systems. One way to fight threats related to errors and omissions is the concept of least privilege. If users are given only the most minimal set of permissions they need to perform their job functions, then it is possible reduce the amount of information that can be accidentally contaminated (Peltier et al., 2005). Another principle that can help is performing adequate and frequent backups of the information on the systems.

**(c) Fraud and Theft:** Information technology is increasingly used to commit fraud and theft. Fraud can be committed by insiders or outsiders (NIST, 1995). The majority of fraud uncovered on computer systems is perpetrated by insiders who are authorized users of a system. Since insiders have both access to and familiarity with the victim computer system, including what resources it controls and where the flaws are, authorized system users are in a better position to commit crimes. An organization's former employees may also pose threats, particularly if their access is not terminated promptly. Many systems can be subject to fraud and theft. For example, individuals working in financial institutions may use a computer to skim small amounts of money from a large number of financial accounts, thus generating a significant sum for their own use. In addition, deposits may be intentionally misdirected. Systems which control access to any resource, are targets, such as time and attendance systems, inventory systems, school grading systems, or long-distance telephone systems. In

addition to the use of technology to commit fraud and theft, computer hardware and software may be vulnerable to theft (NIST, 1995).

**(d) Malicious Hackers:** Malicious hackers gain access to people's computers to commit a variety of computer crimes.

**(e) Malicious Code:** Malicious code is defined as software intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system (USDA, 2011). It is designed with the intent to deny, destroy, modify or impede system configurations, programs or data files. One of the fastest ways to introduce malicious code into a target organization's protected network is by sending the malicious code via e-mail. There are many different types of malicious code but common ones include viruses, worms, and Trojans.

**(f) Denial-of-Service Attacks:** *Denial of Service* (DoS) is an interruption of service either because the system is destroyed or because it is temporarily unavailable. The denial-of-service or DoS attack is designed to either overwhelm the target server's hardware resources or overwhelm the target network's telecommunication lines.

**Table 1: Common denial of service attacks**

| DoS Attack | Description |
|---|---|
| **TCP SYN attack** | The TCP SYN Attack involves transmitting a volume of connections that cannot be completed at the destination. This attack causes the connection queues on the router or the firewall to fill up, thereby denying service to legitimate TCP traffic. |
| **Ping of Death** | A type of DoS attack in which the attacker sends a ping request that is larger than 65,536 bytes, which is the maximum size hat IP allows (IP Packet) |
| **Land.c attack** | This attack involves sending a packet to a device/router with the same IP address in the source address and destination address fields and with the same port number in the source port and destination port fields. This attack can cause a denial of service. |
| **Smurf attack** | Flooding networks with broadcast traffic (ICMP echo requests) such that the network is congested. |
| **Fraggle attack** | Flooding networks with broadcast traffic (UDP echo requests) such that the network is congested. |

**(g) Social Engineering:** Social engineering is a category of security attacks in which someone manipulates others into revealing information that can be used to steal data, access to systems, access to cellular phones, money, or even your own identity (USDA, 2011).This approach is used by many hackers to obtain information valuable to accessing a secure system. Rather than using software to identify security weaknesses, hackers attempt to trick an individual into revealing passwords and other information that can compromise your system security.

A common social engineering scam is phishing. Phishing is a high-tech scam that uses email or websites to deceive users into disclosing credit card numbers, bank account information, social security number, passwords, or other sensitive information (USDA, 2011).

## 2.9 A Conceptual Framework for Information Security Management in Public Universities in Kenya.

### 2.9.1 Framework Introduction

In this section, a conceptual framework for information security management in public universities in Kenya is proposed which is developed from industry best practice recommendations and guidelines in information security management as suggested in various standards, guidelines and literature by information security researchers and practitioners.

The proposed framework served as a guide to the data collection process. It was used to develop the data collection instrument discussed in chapter three, section 3.5. The research adopted the following concepts in developing the framework.

(i) Security mechanisms (defenses) need to be layered to increase the security of a system as a whole (defense in depth strategy). If an attack causes one security mechanism to fail, other mechanisms may still provide the necessary security to protect the system (NIST, 2007). By implementing enough layers of protection the likelihood of compromise is drastically reduced.

(ii) The overall objective of an information security program is to protect the integrity, confidentiality and availability of an institution's information (Peltier et al., 2005).

(iii) Information security management is a process and not a product. Products, such as firewalls, intrusion detection systems, intrusion prevention systems, anti-virus software and vulnerability scanners alone are not sufficient to provide effective Information Security. Effective Information Security incorporates security products, technologies, policies and procedures. The information security management process moves through phases and each phase requiring strategies and activities that will move the process to the next phase.

(iv) A truly effective information security management system integrates processes, people, and technology controls

(v) Computer security requires a comprehensive and integrated approach that considers issues both within and outside the computer security field (NIST, 1996).Careful selection and implementation of managerial, technical and operational controls as well as an understanding of their interdependencies is an important information security management success factor (NIST, 1996)

### 2.9.2 Relating the proposed framework to research questions

The proposed framework for information security management is closely linked to the research questions. This research is designed to answer the following research questions.

(i) What factors determine the overall effectiveness of an information security management system?

(ii) Is there an existing framework for information security management in Kenyan public universities?

(iii) Are information security professionals in public universities in Kenya adhering to best practices in information management?

(iv) What gaps exist between common information security management practices and industry best practices?

As an initial step toward the development of this framework, a list of key ISM best practices based on key literature in information security management (ISO 27001 standard and NIST special publications) was prepared. Most standards tend to be generic and therefore the ISM best practices were selected on the basis of their applicability in institutions of higher learning. The selection of the ISM best practices is closely linked to the first research question which sought to identify the factors that determine the overall effectiveness of an information security management system.

As a final step, the relationships between Information security management objectives and practices were examined. This gave an indication of the relationship between the variables and this culminated in to the formulation of the proposed framework for information security management in public universities in Kenya. This addressed the second research question. The proposed framework was then used to guide the data collection process, including the formulation of the items in the data collection instrument (questionnaire) to investigate information security management systems in public universities in Kenya.

### 2.9.3 Variables

The dependent variable for this study is effective ISMS and the independent variables are ISM best practices derived from standards and key literature in information security management. In determining the variables (factors) that impact on the overall effectiveness of an information

security management system, this study primarily relied on the NIST special publications and the ISO 27001 standard.

### 2.9.4 The Proposed Framework

The proposed framework for information security management shows the relationship between the dependent and independent variables. This framework is presented in Figure 6 below. The framework describes a cycle with five key phases, each phase requiring implementation of certain key ISM processes (ISM best practices), which are important for the overall effectiveness of the information security management system (dependent variable).

**Table 2: ISM best practices and Objectives**

| ISM Phase | ISM Best practices (Independent Variables) | ISM Objectives (dependent variable) |
|---|---|---|
| Planning | Risk Assessment | Effective ISMS ( Protecting confidentiality, Integrity and availability of information) |
| | Organization of information security | |
| | Security policy | |
| | Management support | |
| Implement | Incident response | |
| | Communications and operations security | |
| | Physical and environmental security | |
| | Human resource security | |
| | Access control | |
| | Contingency planning | |
| | cryptography | |
| | Asset classification and control | |
| | Information Systems acquisition development and maintenance | |
| | Patch management | |
| Awareness, training and education | Information security awareness, training and education | |
| Review/ Audit | Information security audits and reviews<br>• Internal & External audits<br>• Self assessments | |
| Maintain | Post audit corrective and preventive actions<br>• Improve, Update & Monitor | |

### 2.9.5 General Description of the proposed Framework

The proposed framework (figure 6) shows the relationship between the dependent variable and the independent variables which have been grouped in five categories. Below is a general description of the various variables which are critical towards achieving an effective information security management system.

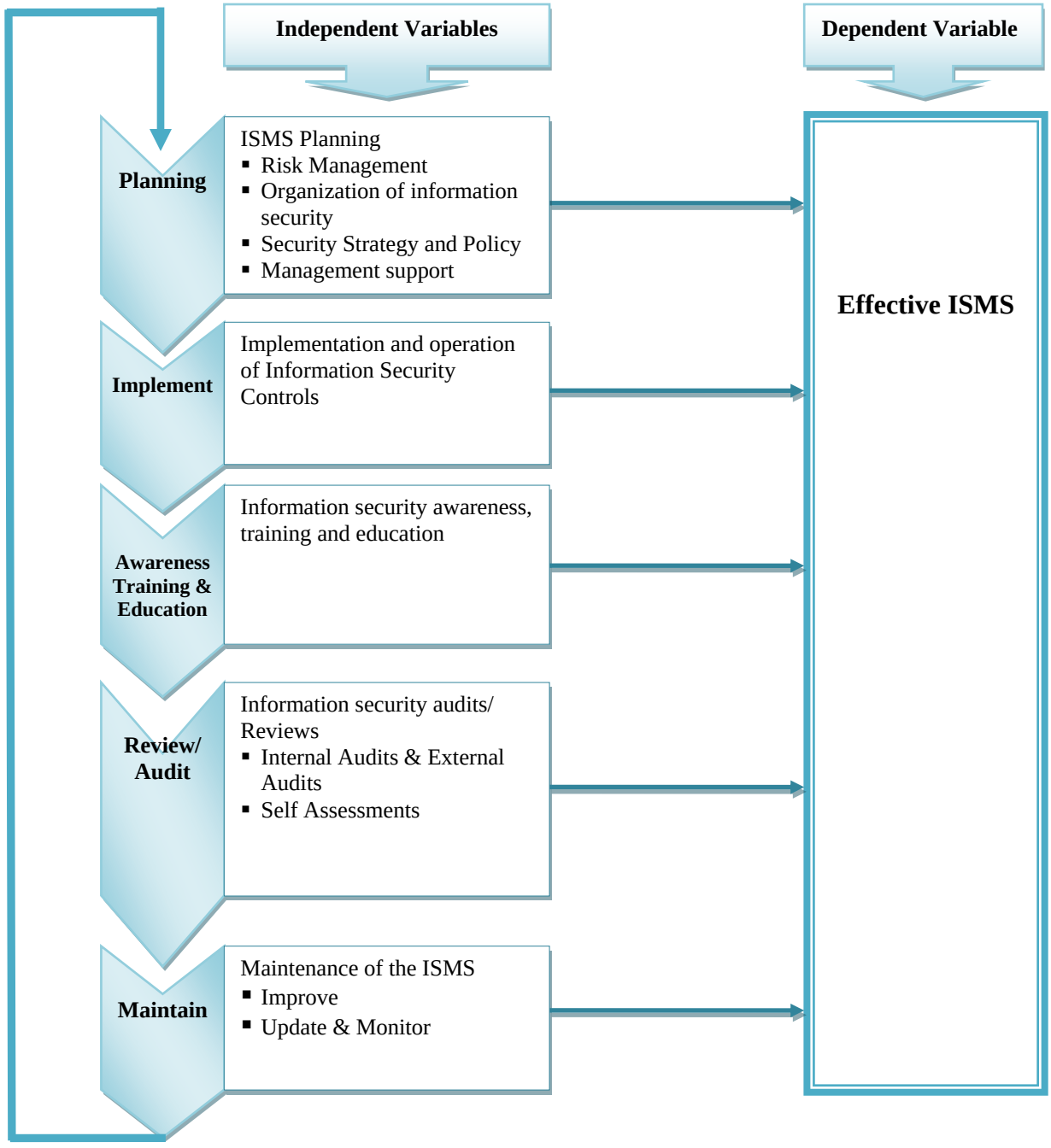


**Figure 6: A Conceptual Framework for Information Security Management in Public Universities in Kenya**

#### 2.9.5.1 Planning Phase

Information security management practices in the planning phase are very vital to the ultimate effectiveness of the ISMS. In this phase of the proposed framework, the major focus is risk assessment, organization of information security and putting in place a security policy and strategy.

**(a) Management approval and support:** It is essential to ensure management involvement and commitment at the planning phase or even before. The role played by management is crucial in the implementation of an effective information security management program. Management should ensure that the proper resources are available and that all employees affected by the ISMS have the proper training, awareness and competency. Without Management support and availability of resources, key ISM best practices identified may not achieve ISM objectives as shown in figure 6.

**(b) Risk assessment:** Risk assessment lies at the heart of effective ISMS. Accurate assessment provides a focus for the implementation of security controls and strategies, and ensures that these controls and strategies are correctly prioritized and cost effective.

#### 2.9.5.2 Implement Phase

The implement phase of proposed framework is concerned with implementation and operation of information security controls. Risk assessment in the planning phase lays the foundation for selection of appropriate security controls.

**(a) Organization of information security**

In control A.6 of the ISO 27001 standard, Management is required to actively support security within the organization through clear direction, demonstrated commitment, explicit assignment, and acknowledgement of information security responsibilities. Information security activities should be co-ordinated by representatives from different parts of the organization with relevant roles and job function. In addition, confidentiality agreements or non-disclosure agreements reflecting the organization's needs for the protection of information should be identified and regularly reviewed (ISO27k Forum, 2011).

**(b) Assets identification and classification**

Public Universities should be in a position to understand what information assets they hold, and to manage their security appropriately. All significant organization assets should be clearly identified and accounted for in an inventory listing, and have assigned owners who are responsible for their appropriate protection (Calder and Watkins, 2008). Rules for the acceptable use of information and other assets associated with information processing facilities should be identified, documented and implemented. Additionally, Information and information processing facilities should be classified in terms of value and criticality to the institution, sensitivity and legal requirements.

**(c) Security policy**

Comprehensive security policy is but one of the key building blocks to an effective ISMS. The policy communicates the security goals to all of the users of information technology assets, the administrators, and the managers. The policy should specify the mechanisms through which these requirements can be met and should have the acceptance and support of all levels of employees within the organization as well as mechanisms for enforcing compliance. According to National Security Agency (2002), a good security policy clearly defines the areas of responsibility for the users, the administrators, and the Managers and should be able to be enforced with security tools where appropriate and with sanctions where actual prevention is not technically feasible.

According to Calder and Watkins (2008), the security policy should be approved by management, published and communicated as appropriate to all employees

**(d) Physical and Environmental Security**

The term physical and environmental security refers to measures taken to protect systems, buildings and related supporting infrastructure against threats associated with their physical environment. The security controls at this level aim to prevent unauthorized physical access or interference to the organization or IT equipment and information assets (Calder and Watkins, 2008). IT equipment and information that require protection should be placed in secure physical areas. Secure areas should have suitable access control to ensure that only authorized personnel have access. Good physical security requires efficient building and facility construction,

emergency preparedness, reliable electrical power supplies, reliable and adequate climate control and effective protection from both internal and external intruders. Management should consider implementing appropriate physical and environmental controls commensurate to risks identified during risk assessment and the value of assets.

According to the ISO 27001 standard, the following controls are crucial in securing systems, buildings and related supporting infrastructures.

- Provision of appropriate protection against fire, water or other reasonably anticipated environmental threats
- Use of appropriate intrusion detection systems such as motion and perimeter alarms, audio and video surveillance.
- Use of manned reception areas or appropriate lock/ID systems to control passage into the restricted areas
- Requirement for authorized personnel to wear visible identification, and to report persons without such identification.

**(e) Access Controls**

Access control deals with authentication and authorization. Logical access to IT systems, networks and data must be suitably controlled to prevent unauthorized use. Passwords are the most often used form of authentication today. The alternatives to passwords include biometrics and smartcards. Poor password selection is frequently a major problem for any system's security. Users should be forced to change their passwords regularly. According to National Security Agency (2002) Passwords should:

- It should be 12 or more characters in length on Windows systems and 8 characters in length on UNIX or Unix based systems
- Include upper and lower case letters, numbers, and special characters and should not consist of dictionary words
- Be changed regularly (every 30 to 90 days)
- Be cracked every month to find users choosing easily guessed or cracked passwords

**(f) Communications and Operations Management**

According to the ISO 27001 standard, the aim of controls in this category is to ensure the correct and secure operation of information processing facilities. Procedures for preventing and dealing with malicious code should be implemented such as installation of anti-virus and anti-spyware software. Such software should be regularly updated. Furthermore, it is necessary to implement mechanisms employing digital certificates for secure communications between communicating entities as well as encryption mechanisms for protecting the confidentiality of the data.

Internal Networks should also be appropriately managed and controlled to ensure that they are protected from threats and to maintain security for the systems and applications using the network. Procedures for logging and monitoring of network activities should be implemented. Information should be backed up and the backup procedures should be tested at appropriate intervals, in accordance with an agreed-upon back-up policy. Security of removable media should also be addressed in addition to their secure disposal when no longer needed

Information involved in electronic messaging should be appropriately protected from unauthorized access, modification or diversion. Electronic messaging includes email, IM and audio-video. According to NIST (2007), the following controls are crucial for secure electronic messaging:

- Implementing cryptographic technologies to protect user authentication and email data
- Patching and upgrading the mail server and mail clients
- Ensuring the general reliability and availability of messaging services
- Stronger levels of authentication and message content protection when using public networks.

**(g) Human Resources security**

According to the ISO 27001 standard, security responsibilities should be addressed at the recruitment stage, in contracts and during an individual's employment. Prior to employment, organizations should ensure that employees, contractors and third party users understand their responsibilities and are suitable for the roles they are considered for to reduce the risk of theft, fraud or misuse of facilities (Arnason and Willet, 2008). Recruits should be adequately screened,

especially for sensitive jobs. During employment, Organizations should ensure that all employees, contractors and third party users are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support organizational security policy in the course of their normal work, and to reduce the risk of human error (Arnason and Willet, 2008).

**(h) Cryptography**

The purpose of cryptography is to protect transmitted information from being read and understood by anyone except the intended recipient. Encryption is the primary mechanism for communications security (Maiwald, 2001). Encryption can also be used to protect information that is in storage by encrypting files.

**(i) Information Systems acquisition, development and maintenance**

Information systems should be developed, acquired, and maintained with appropriate security controls (Calder and Watkins, 2008).

**(j) Contingency planning**

The overall planning for unexpected events is called contingency planning (NIST, 2010). According to NIST (2010), the major components of a contingency plan include an Incident response plan, Business continuity plan and Disaster recovery plan.

The incident response plan (IRP) is a detailed set of processes and procedures that anticipate, detect, and mitigate the impact of an unexpected event that might compromise information resources and assets. Disaster recovery planning is the process associated with the preparation for and recovery from a disaster, whether natural or man-made. A disaster recovery plan (DRP) focuses on restoring operations at the primary site after disasters occur. Business continuity planning is the planning process associated with ensuring that critical business functions continue if a catastrophic incident or disaster occurs. A Business continuity plan (BCP) facilitates establishment of operations at an alternate site, until the organization is able to either resume operations back at its primary site or select a new primary location.

**(k) Patch management**

Patches are additional pieces of code developed to address weaknesses (bugs) in software (NIST, 2005). Regular and timely patching of security issues is generally recognized as critical to maintaining the operational availability, confidentiality, and integrity of information technology (IT) systems (NIST, 2005). Patch management can be the most effective tool used to protect against vulnerabilities and the least expensive to maintain if implemented effectively. It plays an important role in upholding a good enterprise security posture but it should not be treated as the solution for all security vulnerabilities. Patch management is a process that must be done routinely and should be as all-encompassing as possible to be most effective.

**(l) Incident Response**

A well-defined incident response capability helps an institution to detect information security incidents quickly, minimize loss and destruction, identify weaknesses and restore IT operations rapidly (Calder and Watkins, 2008). No security effort is foolproof. Because 100% security is not achievable, incidents will arise and in order to identify and resolve incidents effectively, minimize their business impact and reduce the risk of similar incidents occurring, establishing an incident response capability is critical. An institution should ensure that management responsibilities and procedures are established to ensure a quick, effective and orderly response to information security incidents to allow corrective action to be taken (Calder and Watkins, 2008).

**2.9.5.3 Awareness, training and education Phase**

Security awareness and training is an essential consideration to successfully implement information security policies and to ensure that related controls are working properly. Security awareness efforts are designed to change behavior or reinforce good security practices (NIST, 1998). Training strives to produce relevant and needed security knowledge and skills within the workforce. Training supports competency development and helps personnel understand and learn how to perform their security role. Computer users, and others with access to information resources, cannot be expected to comply with policies that they are not aware of or do not understand. Similarly, if they are not aware of the risks associated with their organization's information resources, they may not understand the need for and support compliance with policies designed to reduce risk. An annual security awareness-training course is an absolute

necessity to keep people up on the latest security information, but equally important are short email updates, newsletters, and other reminders.

Security awareness and training should be focused on the institution's entire user population. Management should set the example for proper IT security behavior within an institution. Promoting awareness can be achieved by:

(i) Intranet websites that communicate and explain information security related policies, standards, procedures, alerts, and special notes

(ii) Awareness videos with enthusiastic endorsements from top management for the security program to supplement basic guidance, such as the importance of backing up files and protecting passwords

(iii) Interactive presentations by security staff to various user groups to market the services of the information security team

(iv) Email updates and newsletters

An IT security awareness and training program should be carefully designed and implemented as part of a successful information security program. The program should be implemented after a needs assessment has been conducted, a strategy has been developed, an awareness and training program plan for implementing that strategy has been completed, and awareness and training material has been developed (NIST, 1998).

Education integrates all of the security skills and competencies of the various functional specialties into a common body of knowledge and adds a multidisciplinary study of concepts, issues, and principles (technological and social).

#### 2.9.5.4 Review/ Audit Phase

The objective of this phase is to review and evaluate the performance (efficiency and effectiveness) of the information security management system. This can be achieved by carrying out an information security audit/review. Information security audit is part of every successful information security management system. The audits are intended to improve the level of information security, avoid improper information security designs, and optimize the efficiency of the security safeguards and security processes. An IS audit can be performed by employees of

the organization itself (internal audit) or by third parties (external audit). The result of the IS audit is the IS audit report, which contains information on the information security status and possibly recommendations for improvements or modifications to IT security safeguards, structures, and processes.

Computer security auditors perform their work though personal interviews, vulnerability scans/ penetration tests, examination of operating system settings, analyses of network shares, and historical data. They are concerned primarily with how security policies - the foundation of any effective organizational security strategy are actually used.

#### 2.9.5.5 Maintain Phase

In the Maintain phase of the proposed framework, changes are made where necessary to bring the ISMS back to peak performance. This phase immediately follows the completion of an information security audit/review. Appropriate corrective and preventive actions are taken to ensure that information security controls are effective.

# CHAPTER THREE

# RESEARCH METHODOLOGY

## 3.1 Overview

This chapter provides information on the procedure used in conducting the study. It provides a description of the activities which were necessary for the completion of the research namely sampling, detailed description of methods used for data collection and data analysis.

## 3.2 Research Design

This research entitled " Information security management in public universities in Kenya: A gap analysis between common practices and industry best practices" is a descriptive survey designed to investigate information security controls and related security management practices in public universities in Kenya, to develop an appropriate framework for effective information security management and to determine and analyze the gaps between actual information security controls and related security management practices and industry best practices in information security management. This study focused on management, operational and technical controls implemented in the public universities.

In this study, a combination of both quantitative and qualitative research approaches was used. The advantage of using a quantitative approach is that variables are easy to measure and analyze. Qualitative research involves studies that do not attempt to quantify their results through statistical summary or analysis and typically involve interviews and observations without formal measurement (Dawson, 2002). The advantage of using qualitative data gathering method in this study is that they are more open to changes and refinement of research ideas as the study progresses (Dawson, 2002). Qualitative research is concerned with subjective assessment of attitudes, opinions and behavior (Kothari, 2004). In this study, the qualitative technique was based on semi-structured interviews to assess the level of importance public universities in Kenya attach to information security, assess the information security policy for adequacy, get important and realistic information on information security awareness among users of information systems, assess attitudes of employees towards the security of information as well as to get their opinions on whether top management is doing enough to ensure security of information.

Another notable strength of the qualitative instruments is that they evoke a more realistic feeling of the research setting which cannot be obtained from statistical analysis and numerical data utilized through quantitative means. By using qualitative research and specifically semi-structured interviews, it was possible to get important and realistic information about IT security awareness (knowledge and skills), senior leadership involvement in tackling security problems, risk management, ownership and accountability for security of campus IT systems, incident handling as well as people's attitudes towards security of information.

### 3.3 The study Population

A research population consists of all individuals or objects of interest to the researcher (Marczyk, DeMatteo and Festinger, 2005). It can also be defined as the total members of a defined class of people, objects, places, groups or events of interest to the researcher. The study population consists of all public universities in Kenya. By the time of analyzing data, there were 7 public universities according to the Commission of Higher Education (CHE). The number has however changed after the government upgraded 15 University colleges to Universities (Appendix B).

### 3.4 Research Sample

A sample is simply a subset of the population (Marczyk et al, 2005). For the purpose of this study, Probability sampling technique was used to select public universities to be included in this study. With probability sampling, each element has a known probability of being included in the sample (Kothari, 2004). The researcher decided to use simple random sampling. In this technique, five public universities out of the 7 public universities in Kenya were selected randomly for inclusion in the sample. The advantages of using simple random sampling in this study include:

1) Ease of assembling the sample.
2) Simple random sampling provides a sample that is highly representative of the population being studied.

The target respondents were directors of ICT, IT security staff, system administrators and Network administrators collectively referred to as "security professionals" who are professionals in the area of information security management and "end-users" of information systems comprising of lecturers, technicians and secretarial staff. In categorizing the respondents, the researcher considered their knowledge and role in information security management in the universities.

The researcher used stratified random sampling to select the respondents from the two strata/ subgroups mentioned above. In stratified random sampling, the population is stratified into a number of nonoverlapping subpopulations or strata and sample items are selected from each stratum (Kothari, 2004). Respondents were selected from each of the subgroups from the sampled universities randomly and questionnaires were mailed to them with a request to mail them back after completion.

Since the security professionals are the people involved directly with information security management in their institutions, any one respondent in this group was in a position to give reliable information regarding information security status in their universities. The researcher therefore targeted two respondents in this subgroup per university. Overall, the researcher targeted a projected sample of approximately 53 respondents.

### 3.5 Data collection

For the purpose of this study, the main method of data collection used was a questionnaire. Two sets of questionnaires were developed, one for "security professionals" and one for "end users" of information systems. In developing the questionnaires, the researcher considered their knowledge and role in information security management in the universities.

The questionnaires were administered to respondents personally or via email in some institutions. The advantage of using the mail questionnaire for the survey is that it is less costly even when the universe is large and is widely spread geographically, it is free from bias of the interviewer and respondents have adequate time to give well thought out responses (Kothari, 2004).

The questionnaires (Appendix B and D) consisted of two parts containing a combination of both open-ended and closed-ended questions. The closed-ended questions had exclusive responses of "Yes", "No" or Don't know responses. The open-ended questions required narrative responses. The first part of the questionnaires was designed to gather institutional information while the remaining section was designed to gather information regarding actual information security controls implemented and related security management practices. The proposed framework for information security management (described further in chapter 2 and in section 2.8) was used to formulate questions to investigate information management systems in public universities in

Kenya and to identify deficiencies/ gaps in the actual security controls implemented and related information security management practices. The distribution of the questions in the questionnaire (Appendix B) with regard to the various information security management practices is shown in the table below.

| **Information security practices** | **Number of questions/items** |
|---|---|
| Risk Assessment | 1 |
| Organization of information security | 2 |
| Asset Management | 1 |
| Security Policy | 7 |
| Incident Response | 1 |
| Communications and Operations Security | 13 |
| Physical and Environmental Security | 2 |
| Personnel Security | 3 |
| Awareness, Training and Education | 3 |
| Patch Management | 1 |
| Hardware Maintenance | 1 |
| Contingency Planning | 4 |
| Access Control | 8 |
| Cryptography | 1 |
| Audit Trails/ Logs | 1 |
| Information security audits/ review | 1 |

The researcher also used semi-structured telephone interviews for qualitative data collection. Semi-structured interviews consist of a list of open-ended questions based on the topic areas the researcher intends to study (Dawson, 2002).

### 3.5.1 Validity

Validity is indicates the degree to which an instrument measures what it is supposed to measure (Kothari, 2004). The researcher carried out a pilot study to ensure that the questionnaire is effective in collecting the relevant information. A preliminary version of the questionnaire was first discussed with the supervisor before piloting. The aim is to improve the validity of the data collection instrument.

The researcher selected randomly four respondents from the University of Nairobi, School of computing and informatics to participate in the pilot study. To establish the content and face validity of the data collection instrument, the respondents were requested to help evaluate the

clarity of the questions and to make the content more comprehensive. Based on their input several items of the initial draft of the questionnaire were restructured to improve comprehension.

### 3.5.2 Reliability

Reliability refers to the consistence, stability or dependability of the data. A measuring instrument is reliable if it provides consistent and dependable results (Kothari, 2004). A reliable measurement is one that if repeated a second time will give the same results as it did the first time. If the results are different, then the measurement is unreliable (Mugenda, 2008).

The evaluation of reliability of the data collection instrument was conducted by means of Kappa coefficient to check the percentage agreement between measures or responses on various items of the questionnaire. The Kappa coefficient for categorical data consists of calculating the proportion of matching replies in two applications of the same instrument. Kappa is always less than or equal to 1. A value of 1 implies perfect agreement and values less than 1 imply less than perfect agreement. Statistical analysis was conducted using SPSS version 20. The values were classified as shown below:

| Kappa | Agreement |
|---|---|
| < 0 | Less than chance agreement |
| 0.01 – 0.20 | Slight agreement |
| 0.21 – 0.40 | Fair agreement |
| 0.41 – 0.60 | Moderate agreement |
| 0.61 – 0.80 | Substantial agreement |
| 0.81 – 0.99 | Almost perfect agreement |

The two data collection instruments (Appendix B and D) used in this study had a combination of both open-ended and closed-ended questions and consisted of two parts. The closed-ended questions had exclusive responses of “Yes”, “No” or Don’t know responses. The open-ended questions required narrative responses. Four randomly selected respondents (two security professionals and two users) from the University of Nairobi, School of computing completed the two questionnaires.

**Computing Kappa Coefficient – Case 1 (Security Professionals)**

Analysis focused on 41 questions. The agreement of "Yes" responses was high (75.6%) and the Kappa coefficient was 0.592 indicating a moderate agreement. This means that security professionals gave to a large extent similar information regarding information security management indicating consistency. This can be attributed to the role of security professionals as regards information security management in their institutions. They are directly involved in information security management.

| First Security Professional * Second Security Professional Crosstabulation | | | | | |
|---|---|---|---|---|---|
| | | | Second Security Professional | | Total |
| | | | Yes | No | |
| First Security Professional | Yes | Count | 31 | 2 | 33 |
| | | % of Total | ***75.6%*** | 4.9% | 80.5% |
| | No | Count | 3 | 5 | 8 |
| | | % of Total | 7.3% | ***12.2%*** | 19.5% |
| Total | | Count | 34 | 7 | 41 |
| | | % of Total | 82.9% | 17.1% | 100.0% |

**Symmetric Measures**

| | Value | Asymp. Std. Error[a] | Approx. T[b] | Approx. Sig. |
|---|---|---|---|---|
| Measure of Agreement Kappa | ***.592*** | .164 | 3.806 | .000 |
| N of Valid Cases | 41 | | | |

In the open-ended questions, moderate agreement (0.41 – 0.60) was obtained in the questions concerning physical and environmental controls, electronic messaging security and password practices.

**Computing Kappa Coefficient – Case 2 (Users)**

Analysis focused on 19 questions. Kappa coefficient was 0.379 indicating a fair agreement.

**Symmetric Measures**

| | Value | Asymp. Std. Error[a] | Approx. T[b] | Approx. Sig. |
|---|---|---|---|---|
| Measure of Agreement Kappa | **.379** | .184 | 2.124 | .034 |
| N of Valid Cases | 19 | | | |

## 3.6 Research Procedure

The target respondents were directors of ICT, IT security staff, system administrators and Network administrators collectively referred to as "security professionals" and "end-users" of information systems comprising of lecturers, technicians and secretarial staff.

The participants were given a questionnaires comprising of two sections which required 15-25 minutes to complete. The questionnaires were administered to Participants personally or via email in some institutions. The Participants were required to complete the questionnaires and email them back to the researcher. In some institutions, semi-structured interviews were administered to respondents to get more in-depth information. A list of specific questions was prepared by the researcher on important information security topics/areas in line with industry best practices.

## 3.7 Data Analysis

This study generated both quantitative and qualitative data. Completed questionnaires were checked, coded and entered in to an excel database. Descriptive statistics was used for data analysis. Data was analyzed using SPSS (Statistical Package for the Social Sciences) version 20 to arrive at frequencies, percentages and finally cumulative percentages which were thereafter tabulated and also presented in pie charts and graphs using Microsoft excel.

Furthermore, binomial test using SPSS was used to evaluate the relationship between the dependent variable and the independent variables. A one sample binomial test allowed the researcher to test whether the proportion of "yes" responses significantly differs from a hypothesized value of 20%, and therefore test null hypothesis that the proportion of security professionals who indicate their institution has implemented a certain security factor is equal to 20%. A test proportion of 20% was chosen because it indicates that at least that factor was implemented and that the factor is considered important towards achieving an effective information security management system (dependent variable).

## 3.8 Ethical Considerations

As this study requires the participation of human respondents, certain ethical issues were addressed. The consideration of these ethical issues was necessary for the purpose of ensuring the privacy of the participants. Among the significant ethical issues that were considered in the

research process include consent and confidentiality.

Before completing the questionnaire Subjects were required to read the informational cover letter (Appendix A). The researcher explained important details about this study to enable the respondents to understand the importance of their role in the completion of the research. The researcher has also explained the purpose of the research and also informed them that the survey was anonymous. Only an identification number (ID) was required to distinguish various responses. The respondents were also advised that they could withdraw from the study even during the process. With this, the participants were not forced to participate in the research. The confidentiality of the participants was also ensured by not disclosing their names or personal information in the research. Only relevant details that help in answering the research questions are included. The researcher left the respondents with his contact information in case they have any questions or concerns

# CHAPTER FOUR

# RESULTS AND DISCUSSION

## 4.1 Introduction

In this chapter, data collected from the sample population of 31 respondents chosen from five public universities is analyzed. The study was largely completed by directors of ICT, IT security staff, system administrators and Network administrators collectively referred to as information security professionals and end-users of information systems comprising of lecturers, technicians and secretarial staff (described further in chapter 3, and in section 3.4). Two sets of questionnaires were used, one for "information security professionals" and one for "end users" of information systems. The questionnaires were administered to respondents personally or via email in some institutions. The overall response rate was 58.5%.

**Table 3: Job Role of respondents and percentage responses (Security Professionals)**

| Job Role (Respondents) | Target | Received | % Response rate |
|---|---|---|---|
| Directors of ICT | 4 | 2 | 50% |
| ICT Security officer | 1 | 1 | 100% |
| Security Administrators | 2 | 1 | 50% |
| Network Administrator | 4 | 2 | 50% |
| **TOTAL** | **11** | **6** | **54.5%** |

**Table 4: Job Role of respondents and percentage responses (End users)**

| Job Role (Respondents) | Target | Received | % Response rate |
|---|---|---|---|
| Lecturers | 15 | 10 | 66.7% |
| Tutorial fellow | 3 | 2 | 66.7% |
| Technicians/ Technical Support staff | 6 | 3 | 50% |
| Secretarial staff/Administrative officer | 10 | 6 | 60% |
| MIS officer/ MIS Manger | 4 | 2 | 50% |
| Webmaster/ Web Developer | 4 | 2 | 50% |
| **TOTAL** | **42** | **25** | **59.5%** |

This study generated both quantitative and qualitative data. Both sets of questionnaires were analyzed independently. Descriptive statistics was used for analysis. Data was analyzed using SPSS (Statistical Package for the Social Sciences) to arrive at frequencies, percentages and finally cumulative percentages which were thereafter tabulated, and also presented in pie charts and graphs using Microsoft excel.

## 4.2 Quantitative analysis

### 4.2.1 Risk Assessment

In the plan phase of the proposed framework for information security management in public universities in Kenya, risk management was identified as an important process that focuses on identifying threats, vulnerabilities, and attacks to determine what controls can protect information. Proper information security is only possible on the basis of sound risk analysis. Surprisingly, when asked whether their institutions had undertaken risk assessment, security professionals indicated that their institutions had not carried out risk analysis to identify risks to their information assets as shown in figure 7 below.

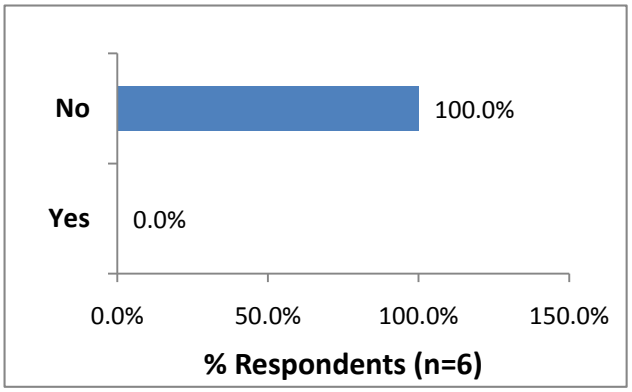


**Figure 7: Has your institution undertaken risk assessment**

### 4.2.2 Contingency planning

Major components of a good contingency plan include an Incident response plan, Business continuity plan and Disaster recovery plan (implementation phase). According to the majority of the security professionals, contingency planning had not been adequately addressed. Majority of the security professionals (50%) indicated that their institutions had not implemented a disaster recovery plan (DRP) as shown in figure 8. Furthermore, no public university had implemented a

business continuity plan. In addition, majority of the security professionals (83.3%) indicated that their institutions had not implemented an IRP and as shown in the figure below.

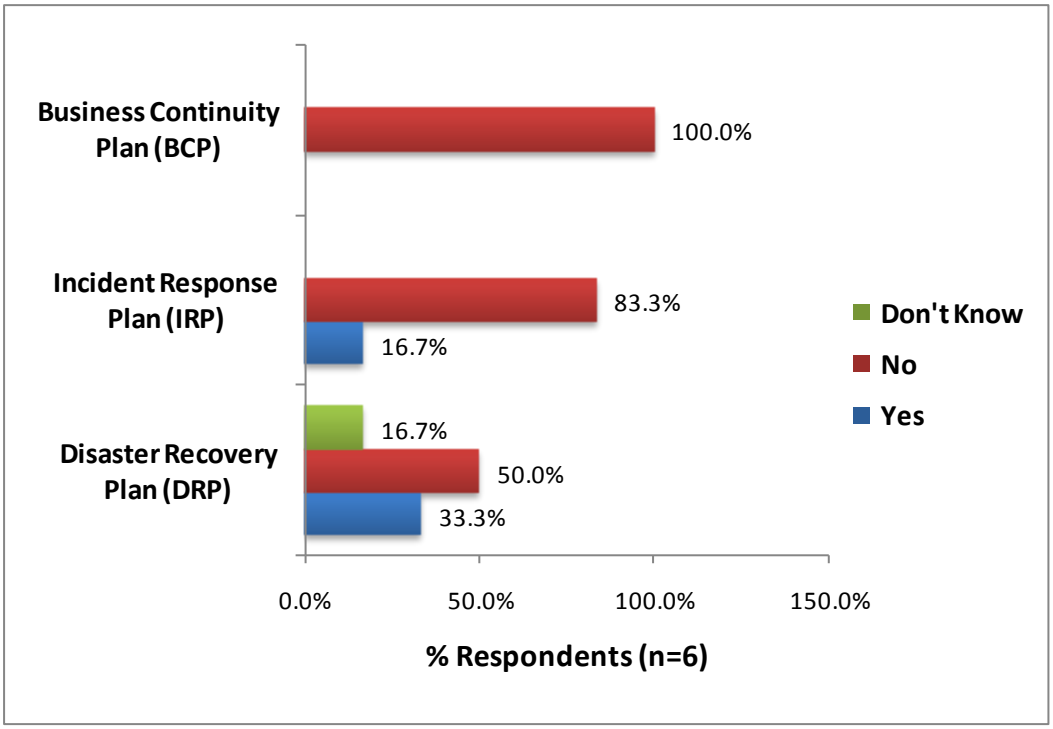


**Figure 8: Implementation status of contingency planning according to security professionals**

### 4.2.3 Information security policy

The cornerstone of effective information security architecture is a well written security policy. The main purpose of a security policy is to inform the users, the administrators and the managers of their obligatory requirements for protecting technology and information assets. The policy should be approved by management, published and communicated, as appropriate to all employees. According to most security professionals (100%), a majority of the institutions have implemented an information security policy. However when users were asked questions relating to status of the information security policy, it was clear that the policy had not been communicated to a great number of users (72%) as shown in table 5. Furthermore, majority of the users have not read their institution's information security policy and they don't understand it either as shown in the table below. Regarding whether the security policy is published on their intranet, only 22.7% indicated that it had actually been published.

**Table 5: Status of Information Security Policy as described by end users (n=25)**

| | Yes | No | Don't Know |
|---|---|---|---|
| Information security policy has been communicated to all employees and relevant external parties | 28% | 72% | - |
| Information security policy has been approved by top management | 34.8% | - | 65.2% |
| Violation of information security policy is punishable | 62.5% | 12.5% | 25% |
| I have read and understood my institution information security policy | 8% | 92% | - |
| Information security policy is published/ available online through our website/intranet | 22.7% | 27.3% | 50% |

### 4.2.4 Asset classification and control

To maintain appropriate protection of organization assets, all assets should be clearly identified and an inventory drawn up and maintained. Rules for the acceptable use of information and assets should be implemented. A majority (83.3%) of security professionals indicated that their institutions had indeed identified and drawn an inventory of their institution assets as shown in table 6. 16.7% however indicated that their institutions had not as shown in the table below.

**Table 6: Assets are clearly identified and an inventory of important assets drawn up and maintained**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Yes | 5 | 83.3 | 83.3 | 83.3 |
| | No | 1 | 16.7 | 16.7 | 100.0 |
| | Total | 6 | 100.0 | 100.0 | |

### 4.2.5 IT Security Technologies

Network Firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), VPN for remote access, and Centralized backup systems are key security technologies implemented in most public universities as shown in figure 9.

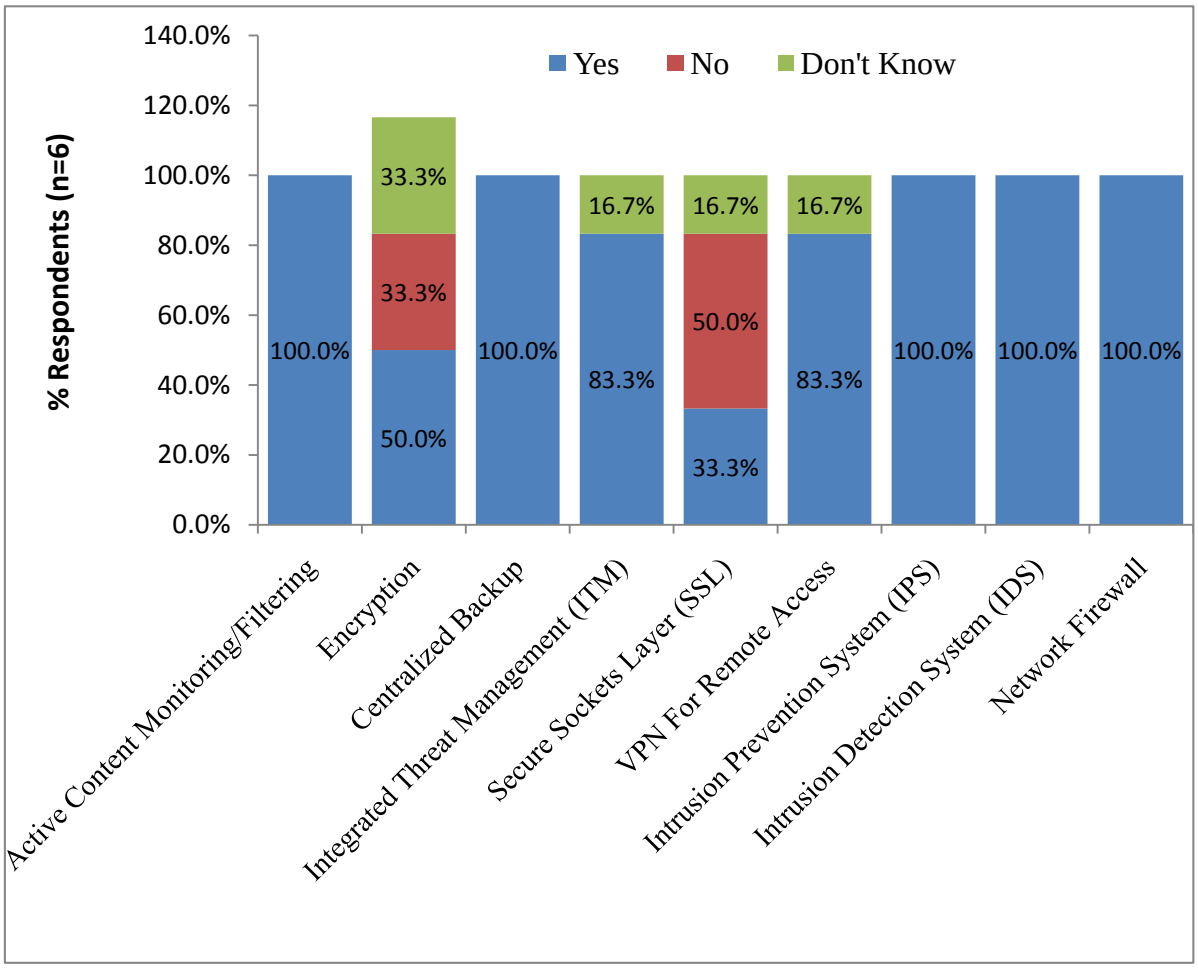


**Figure 9: Information security technologies adopted in public universities according to security professionals**

### 4.2.6 Password Security

Poor password selection is frequently a major problem for any system's security. Users should be forced to change their passwords regularly and the passwords should not be easy to guess. All institutions responding to the survey reported using passwords for authentication. However, only 50% of the security professionals indicated that their institutions had put in place a process to ensure users select good/strong passwords as shown in figure 10.

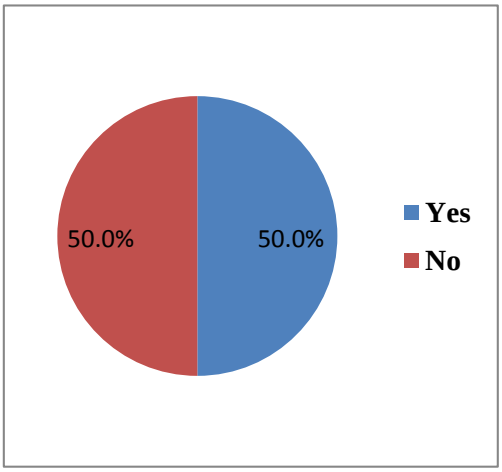


**Figure 10: Is there a process in place that ensures users select good passwords (n=6)**

Survey results also indicate that some users did not understand the characteristics of a good password. A majority of the users however know the characteristics of a good password. 96% of users indicated that a good password is one that includes upper and lower case letters, numbers and special characters. However, 48% of the users preferred using a password they can remember such as their name. Such a password would be easy to guess and does not conform to best practices in password selection. A password is a critical line of defense and therefore good security practices in the selection of passwords will keep information secure.

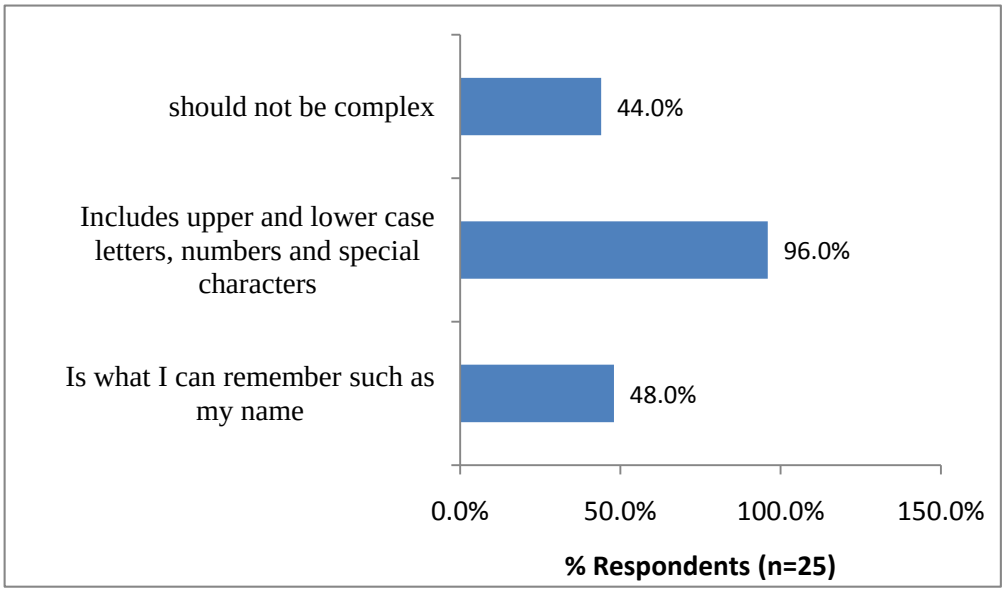


**Figure 11: Characteristics of a good password according to users**

When asked when they changed last changed their passwords, it emerged that 12.0% of the users had never changed their passwords. 24.0% had changed it in the last one month, 16.0% in the last four months, 12.0% in the last six months and 24.0% in the last one year as shown in the figure 12 below. This clearly indicates that although password policies are in place, they have not been communicated or enforced in most of the public universities.

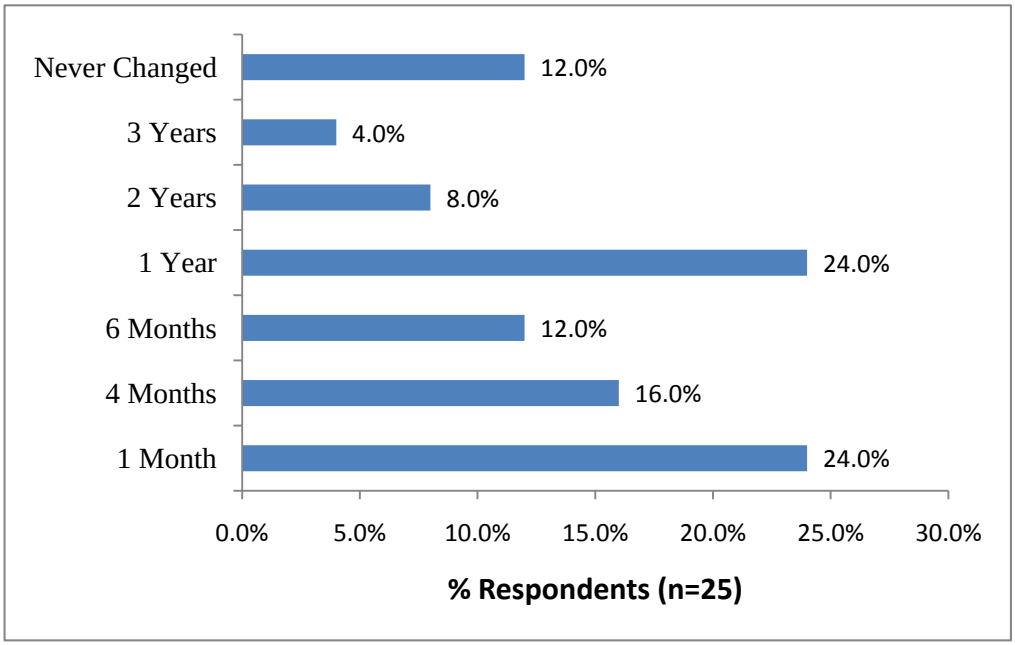


**Figure 12: When did you last change your password**

### 4.2.7 Information security incident reporting and management

Survey results indicate that majority of the public universities have not implemented information security incident reporting and management procedures. When users were asked whether their institutions had a formal IT security incident handling procedure, majority of the respondents (72%) said they didn't have as shown in figure 13. Information Security incidents can never be predicted and therefore procedures should be established to ensure a quick, effective and orderly response to information security incidents to allow corrective action to be taken.

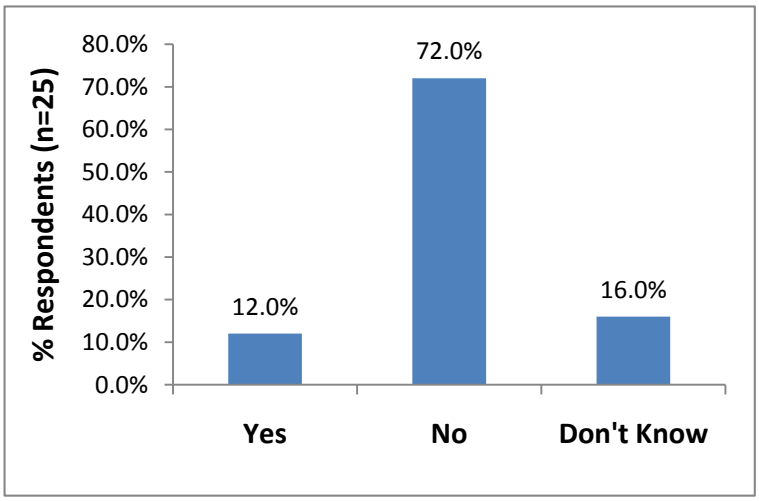


**Figure 13: Do you have a formal IT security incident handling procedure in your institution**

### 4.2.8 Information Security Awareness, Training and Education

An important aspect of a successful information security program is information security awareness, training and education. Surprisingly, only 21.7% of the users indicated that a formal information security awareness program for staff existed in their institutions as shown in Figure 14.

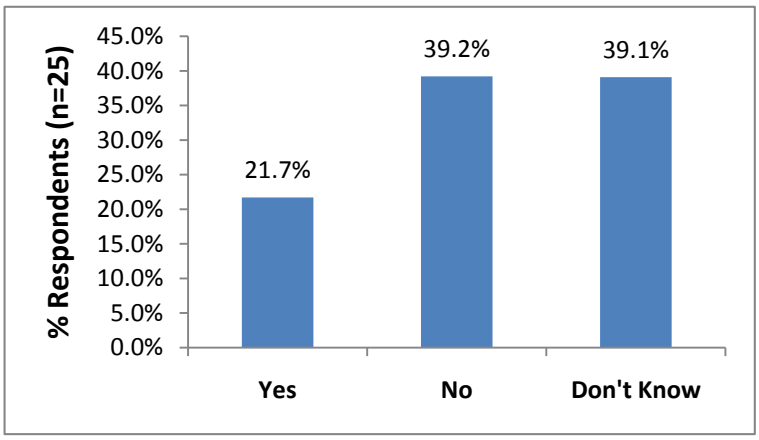


**Figure 14: My Institution has an IT Security awareness program for staff (n=25)**

Furthermore, only 16% of the users indicated that they had received training on information security as shown in figure 15. Without proper security awareness training, users may not be aware of security risks and how these risks may be overcome within their day-to-day job functions.

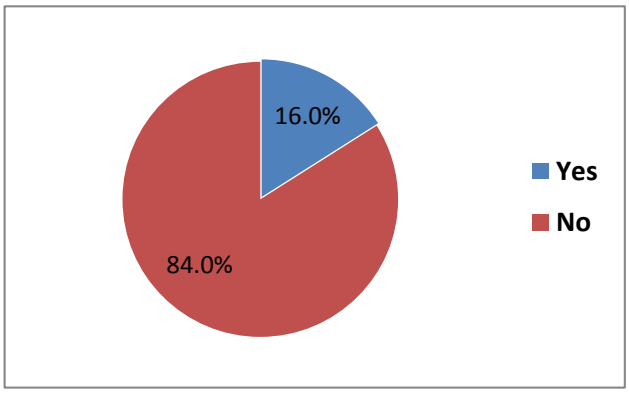


**Figure 15: Have you been trained in information security (n=25)**

### 4.2.9 Organization of information security

Management is required to actively support security within the organization through clear direction, demonstrated commitment, explicit assignment, and acknowledgement of information security responsibilities (Implement phase). The security professionals indicated that there is a person in charge of day-to-day management of IT Security in their university. This is a clear demonstration of the growing importance of the information security function in public universities in Kenya.

**Table 7: Title of officer incharge of IT Security according to security professionals**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Chief ICT Officer (Security) | 3 | 50.0 | 50.0 | 50.0 |
| | Security Administrator | 2 | 33.3 | 33.3 | 83.3 |
| | Network Security Officer | 1 | 16.7 | 16.7 | 100.0 |
| | Total | 6 | 100.0 | 100.0 | |

### 4.2.10 Human Resource Security

Security responsibilities should be addressed at the recruitment stage, in contracts and during an individual's employment (implement phase). Majority of the security professionals (83.3%) indicated that security roles and responsibilities are not included in terms and conditions of employment in their university as shown in the figure 16.

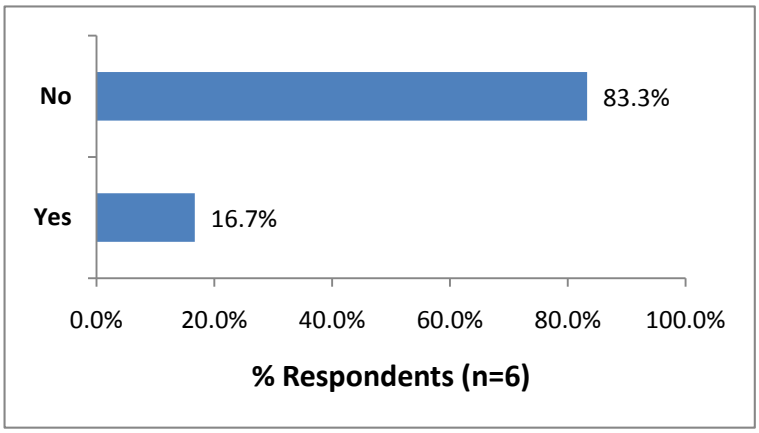


**Figure 16: Addressing security roles and responsibilities at recruitment stage**

In addition the security professionals indicated that all employees/contractors who had privileged access to information systems had not undergone background security investigations as shown below.

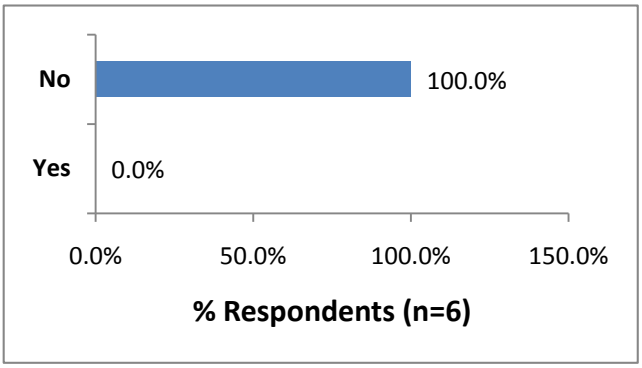


**Figure 17: Addressing security roles and responsibilities (employees and contractors)**

### 4.2.11 Communications and operations management

**Controls against malicious code**: Appropriate controls should be implemented for prevention, detection and response to malicious code, including appropriate user awareness. Institutions should make Use of anti-virus software to stop malicious code from entering their systems. The Antivirus should be updated most frequently.

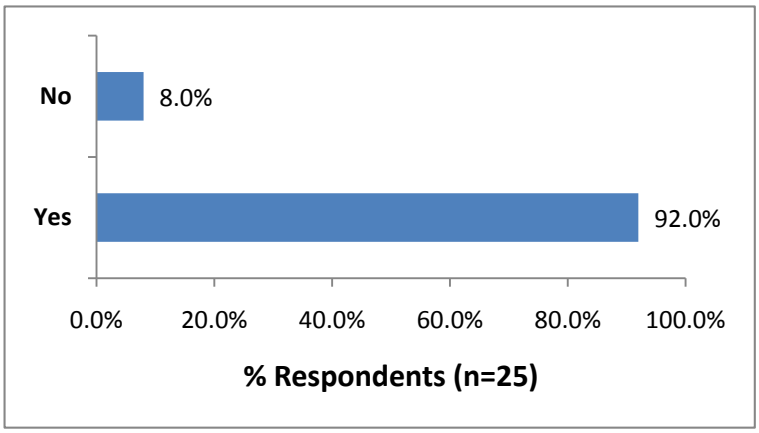


**Figure 18: Do you have protection against viruses (malicious code)**

When users where asked whether they have antivirus installed on their machines, a majority (92%) of the users indicated that they had antivirus protection installed on their operating systems as shown in figure 18. In addition, 80% were using commercial versions (Kaspersky, Norton and McAfee) which are updated automatically. 9.1% of the users indicated that they use free versions of antivirus (Avira and AVG). Eight percent of the users however did not antivirus protection on their computers.

**Table 8: Is the antivirus you are using open source, free or commercial (n=25)**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Commercial | 20 | 80.0 | 90.9 | 90.9 |
| | Free Version (AVG, Avira) | 2 | 8.0 | 9.1 | 100.0 |
| | Total | 22 | 88.0 | 100.0 | |
| Missing | 99 | 3 | 12.0 | | |
| Total | | 25 | 100.0 | | |

**Electronic Messaging security:** Information involved in electronic messaging should be appropriately protected. Majority (50%) of security professionals indicated that their institution has adequately implemented security for electronic messaging as shown in figure 19.

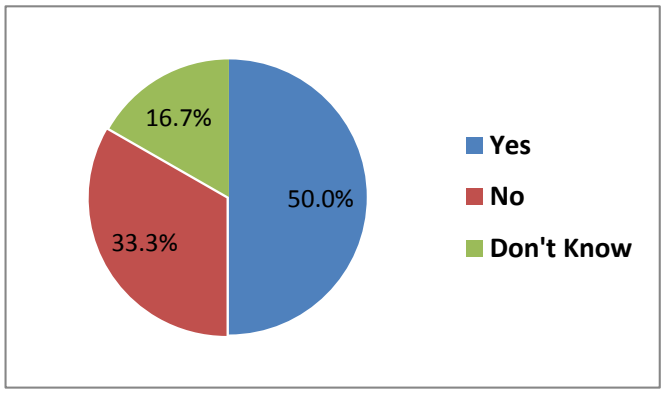


**Figure 19: Has you institution implemented electronic messaging security (n=6)**

Furthermore, security professionals indicated that their institutions were using controls such as firewalls, encryption and mail scanners. Some institutions however are only using firewall meaning incoming and outgoing mail is not checked for malicious content.

**Table 9: Electronic Messaging Security Measures (n=6)**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Firewall | 2 | 33.3 | 33.3 | 33.3 |
| | Use of passwords and Encryption, firewall | 2 | 33.3 | 33.3 | 66.7 |
| | Mail Scanning, IP Based Login, Fail2Ban, SMTP restrictions, Blocking unused ports | 1 | 16.7 | 16.7 | 83.3 |
| | Mail Filtering | 1 | 16.7 | 16.7 | 100.0 |
| | Total | 6 | 100.0 | 100.0 | |

### 4.2.12 Barriers to IT Security

Enforcement of policies was cited as the major barrier to IT security according to a majority of security professionals (66.7%) in the public universities followed by senior management support and Lack of resources as shown in figure 20. Lack of awareness and absence of policies ranked fourth and fifth respectively.

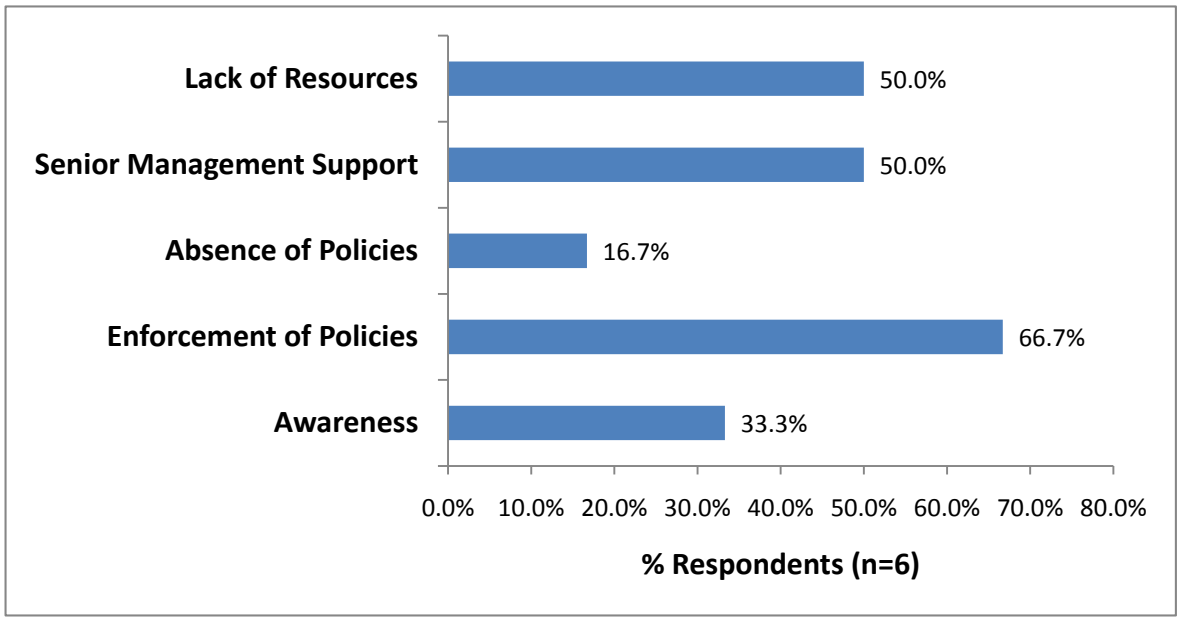


**Figure 20: Major Barriers to IT Security**

### 4.2.13 Information security audits/ reviews

Information security audits/reviews form part of every successful information security management system (Evaluate/Review phase). The audits are intended to improve the level of information security, avoid improper information security designs, and optimize the efficiency of the security safeguards and security processes. An IS audit can be performed by employees of the organization itself (internal audit) or by third parties (external audit). Fifty percent (50%) of the security professionals indicated that their institutions carry out information security audits/ reviews on annual basis while 50% indicated that their institutions don't carry out information security audits as shown in figure 21.

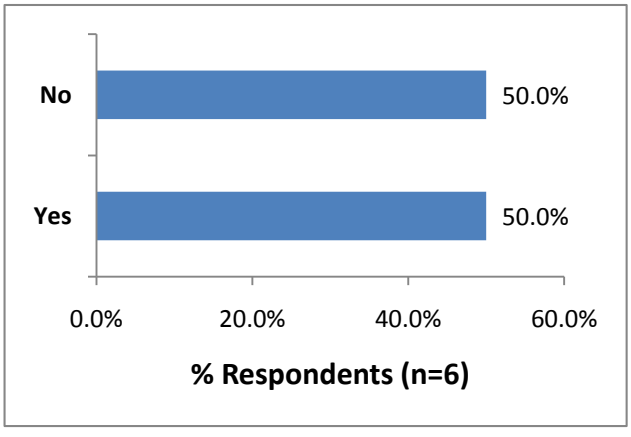


**Figure 21: Does your institution carry out regular information security Audits/ Reviews**

### 4.2.14 Access controls

When asked whether access rights of employees are terminated upon termination of employment, majority (66.7%) of the security professionals indicated that their institutions do not terminate access rights of employees who have left employment.

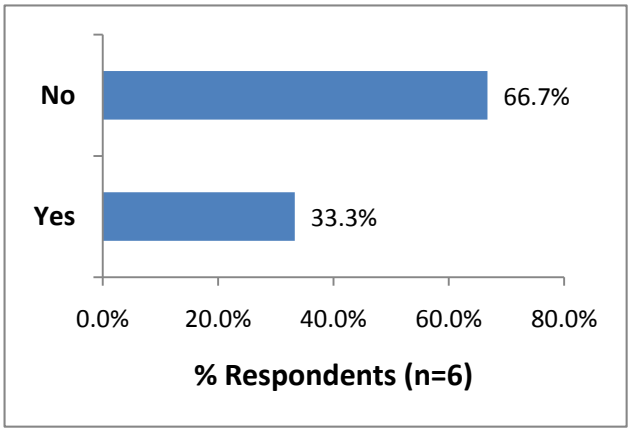


**Figure 22: Are access rights of employees terminated upon termination of employment**

### 4.2.15 Security threats and breaches

Respondents were asked if their institution had been compromised in the last two years. Majority (50%) of the users indicated that their institutions had indeed been compromised. 41.7% of the users (respondents) however did not know whether their institutions had experienced a security breach in the last two years.

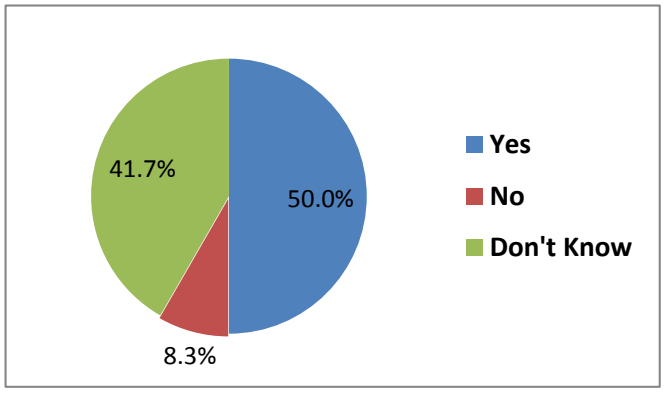


**Figure 23: Has your institution been compromised in the last 2 years (n=25)**

## 4.3 Qualitative analysis

### 4.3.1 Physical and environmental security

Respondents (security professionals) were asked whether physical security for offices, rooms and facilities had been designed and applied and if they were applied to state the controls implemented. Most of the responses were "Yes". Additionally the respondents mentioned physical controls implemented as follows.

- Security checks/ Security Guards/ Manned gates
- Access control system, locks and alarms - ICT Building
- Identification tags
- Burglar proof doors/ Grills

**Controls against Fire, Floors, Earthquakes and student unrest**

As shown in the table below, most of the public universities have implanted controls against fire. Only University A however has implemented controls against floods

**Table 10: Controls implemented against Fire, Floods, earthquake and student unrest**

| University | Controls implemented against Fire, Floods, earthquake and student unrest |
|---|---|
| University A | Fire detectors, raised floor and security guards |
| University B | Fire suppression systems |
| University C | Fire Suppression systems |
| University E | Fire suppression systems, Burglar doors |

### 4.3.2 Communications and operations management

**Electronic messaging security**

Respondents were asked the measures they have implemented to secure electronic messages. The following were the responses according to the security professionals in the Public universities. University E uses only a firewall which means that electronic mails are not scanned for malicious content

**Table 11: Electronic messaging security implemented by various Universities**

| University | Electronic Messaging Security |
|---|---|
| University A | Security professionals in University A indicated that they use a Linux mail server. Security controls implemented: mail scanning (ClamAV), IP based login, Fail2ban, SMTP Restrictions, Blocking unused ports using internal firewall, username and password, encryption |
| University B | Firewall, Passwords and Encryption |
| University C | Mail scanning/Filtering |
| University E | Firewall |

**Controls Against malicious code (Viruses)**

When users were asked whether they had protection against malicious code, most of them responded with yes and also stated the types of antivirus systems installed on their machines. In University C, some users were using free antivirus versions. These free versions of antivirus are not reliable.

**Table 12: Antivirus Systems Implemented in various universities**

| University | Antivirus used |
|---|---|
| University A | Commercial – MaCAfee. Updated automatically |
| University B | Commercial – Norton. Updated automatically |
| University C | Commercial – MaCAfee. Updated automatically. Some users had Avast Free version |
| University D | Some users are using personal copies of Kaspersky |
| University E | Commercial – MaCAfee. Updated automatically |

## 4.4 Analysis of the relationship between dependent variable and independent variables

With regard to information security management practices, this study attempts to investigate the ISM best practices implemented by information security practitioners in Kenyan public universities towards achieving effective ISMS. This provides the basis for refining the proposed framework for effective information security management presented in figure 6 and to determine the most significant factors necessary to achieve effective information system management system (dependent variable).

### (a) Risk Assessment

This section sought to explore the relationship between risk assessment and the dependent variable (effective ISMS). The goal was to show whether there exists any relationship between risk assessment and effective information security management. As shown in figure 7, none of the public universities had carried out risk assessment to determine appropriate controls to protect information assets according to the security professionals. The results indicate that information security professionals do not consider risk assessment as a critical factor towards achieving an effective information security management program

### (b) Information security policy (ISP)

Binomial test using SPSS was used to evaluate whether there exists any relationship between information security policy and an effective information security management system. There were seven questions on information security policy but there was one main question. The question aimed at investigating whether a documented information security policy exists. The goal of the test was essentially to determine if information security policy is considered a significant factor towards achieving an effective information security management system.

***Question: Does your institution have an information security policy?***

This question investigates whether public universities have a documented information security policy and whether information security policy has a significant contribution to effective ISMS (dependent variable). Most security professionals in public universities indicated that their institutions had implemented an information security policy an indication that information security policy a very important factor for an effective information security management system.

**Hypothesis testing**

The null and alternative hypotheses are as follows:

Null hypothesis, $H_0$: P = 0.2

Alternative hypothesis, $H_1$: P > 0.2

Where P means proportion of security professionals who indicate their institution has implemented security policy

**Table 13: Binomial Test of information security policy factor**

| | | Category | N | Observed Prop. | Test Prop. | Exact Sig. (1-tailed) |
|---|---|---|---|---|---|---|
| My institution has an IT security policy | Group 1 | Yes | 5 | .8 | .2 | .002 |
| | Group 2 | Don't Know | 1 | .2 | | |
| | Total | | 6 | 1.0 | | |

From the results, p-value of 0.002 is significantly less than 0.05, meaning that the researcher should reject the null hypothesis that proportion of security professionals who indicate their institution has implemented security policy is equal to 20%, in favor of the alternative hypothesis that proportion of security professionals who indicate their institution has implemented security policy is greater than 20%. This means that Information security policy is a significant factor towards achieving an effective information security management system.

**(c) Asset classification and control**

Binomial test using SPSS was used to evaluate whether there exists any relationship between asset classification and control and an effective information security management system (dependent variable). The goal of the test was essentially to determine if asset classification and control is a significant factor towards achieving an effective information security management system. There was one main question.

***Question: Are all assets clearly identified and an inventory of all important assets drawn up and maintained?***

This question investigates whether public universities have an up-to-date inventory of information assets and to determine whether they consider asset classification and control an

important factor towards achieving an effective information security management system. As shown in Table 6, majority of the security professionals (83.3%) indicate that an inventory of important information assets is maintained. 16.7% of security professionals indicate that their institution does not have a register of important information assets.

**Hypothesis testing**

The null and alternative hypotheses are as follows:

Null hypothesis, $H_0$: P = 0.2

Alternative hypothesis, $H_1$: P > 0.2

Where P means proportion of security professionals who indicate their institution has implemented asset classification and control

**Table 14: Binomial Test of asset classification and control factor**

| | | Category | N | Observed Prop. | Test Prop. | Exact Sig. (1-tailed) |
|---|---|---|---|---|---|---|
| Assets are clearly identified and an inventory of important assets drawn up and maintained | Group 1 | Yes | 5 | .8 | .2 | .002 |
| | Group 2 | No | 1 | .2 | | |
| | Total | | 6 | 1.0 | | |

**(d) Contingency planning**

Binomial test using SPSS was used to evaluate whether there exists any relationship between contingency planning and an effective information security management system. Four questions were asked in relation to this factor but there was one major question.

***Question: Have plans been developed and implemented to maintain or restore operations and ensure availability of information at the required level and in the required time scales following interruption to, or failure of, critical business processes?***

This question investigates whether public universities have implemented procedures to restore operations whenever disruption of critical business services occurs and to evaluate whether security professionals consider contingency planning a significant factor towards achieving effective ISMS

**Hypothesis testing**

The null and alternative hypotheses are as follows:

Null hypothesis, $H_0$: P = 0.2

Alternative hypothesis, $H_1$: P > 0.2

Where P means proportion of security professionals who indicate their institution has implemented contingency planning.

**Table 15: Binomial Test of contingency planning factor**

| | | Category | N | Observed Prop. | Test Prop. | Exact Sig. (1-tailed) |
|---|---|---|---|---|---|---|
| Have plans been developed and implemented to maintain or restore operations | Group 1 | Yes | 4 | .7 | .2 | .017 |
| | Group 2 | No | 2 | .3 | | |
| | Total | | 6 | 1.0 | | |

From the results, p-value of 0.017 is less than 0.05, meaning that the researcher should reject the null hypothesis in favour of the alternative hypothesis that proportion of security professionals who indicate their institution has implemented contingency planning is greater than 20%. This means that Contingency planning is a significant factor towards achieving an effective information security management system.

**(e) Organization of information security**

This section sought to explore whether there is a relationship between organization of information security and effective ISMS. As shown in Table 7, all the public universities had an officer in charge of the day-to-day management of IT security according to security professionals. This is an indication that organization of information security is an important factor towards achieving an effective information security management system.

**(f) Information security awareness, training and education**

Binomial test using SPSS was used to evaluate whether there exists any relationship between information security awareness, training and education and effective information security management system. Three questions were asked in relation to this factor but there was one major question.

***Question: Has your institution implemented a formal IT Security awareness program for employees?***

This question investigates whether public universities have an information security awareness program and to evaluate whether security professionals consider information security awareness and training a significant factor towards achieving effective ISMS

**Hypothesis testing**

The null and alternative hypotheses are as follows:

Null hypothesis, $H_0$: P = 0.2

Alternative hypothesis, $H_1$: P > 0.2

Where P means proportion of security professionals who indicate their institution has implemented an information security awareness program.

**Table 16: Binomial Test for information security awareness factor**

| | | Category | N | Observed Prop. | Test Prop. | Exact Sig. (1-tailed) |
|---|---|---|---|---|---|---|
| My Institution has IT security Awareness program for staff | Group 1 | Yes | 5 | .8 | .2 | .002 |
| | Group 2 | No | 1 | .2 | | |
| | Total | | 6 | 1.0 | | |

From the results, p-value of 0.002 is significantly less 0.05, meaning that the researcher should reject the null hypothesis that proportion of security professionals who indicate their institution has implemented security awareness program is equal to 20%, in favour of the alternative hypothesis that proportion of security professionals who indicate their institution has implemented information security awareness program is greater than 20%. This means that an information security awareness program is considered a significant factor towards achieving an effective information security management system.

**(g) Access control**

Binomial test using SPSS was used to evaluate whether there exists any relationship between access control and effective information security management system. Eight questions were asked in relation to this factor but there was one major question.

***Question: Is there a process in place that ensures users follow good security practices in the selection and use of passwords?***

This question investigates whether public universities have a process in place to ensure the selection of strong passwords and to evaluate whether security professionals consider access control a significant factor towards achieving effective ISMS.

**Hypothesis testing**

The null and alternative hypotheses are as follows:

Null hypothesis, $H_0$: P = 0.2

Alternative hypothesis, $H_1$: P > 0.2

Where P means proportion of security professionals who indicate their institution has implemented password guidelines to ensure selection of strong passwords. Access control is concerned with identification and authentication.

**Table 17: Binomial Test of access control factor**

| | | Category | N | Observed Prop. | Test Prop. | Exact Sig. (1-tailed) |
|---|---|---|---|---|---|---|
| Password guidelines | Group 1 | Yes | 3 | .5 | .2 | .099 |
| | Group 2 | No | 3 | .5 | | |
| | Total | | 6 | 1.0 | | |

The p-value (0.099) is less than 0.1 but greater than 0.05 meaning there is weak evidence in favour of the alternative hypothesis that the proportion of security professionals who indicate their institution has implemented password guidelines is greater than 20%, concluding that there is a relationship between access control and effective ISMS although the relationship is a weak one according to security professionals.

### (h) Incident Response

Binomial test using SPSS was used to evaluate whether there exists any relationship between incident response capability and effective information security management system. One question was asked in relation to this factor.

***Question: Has your institution implemented an incident response plan (IRP)?***

This question investigates whether public universities have implemented procedures for incident reporting and management and thus evaluate whether security professionals consider incident response planning a significant feature towards achieving effective ISMS.

**Hypothesis testing**

The null and alternative hypotheses are as follows:

Null hypothesis, $H_0$: P = 0.2

Alternative hypothesis, $H_1$: P > 0.2

Where P means proportion of security professionals who indicate their institution has ***not*** implemented an incident response plan (IRP).

**Table 18: Binomial Test of incidence response capability factor**

| | | Category | N | Observed Prop. | Test Prop. | Exact Sig. (1-tailed) |
|---|---|---|---|---|---|---|
| Has institution implemented an incident response plan (IRP) | Group 1 | No | 5 | .8 | .2 | .002 |
| | Group 2 | Yes | 1 | .2 | | |
| | Total | | 6 | 1.0 | | |

The significance (p) value of .002 is less than 0.05 therefore the researcher should reject the null hypothesis in favour of the alternative hypothesis that the proportion of information security professionals who indicate that their institutions have not implemented and incident response plan (IRP) is greater than 20%, concluding that there is a weak relationship between IRP and effective ISMS.

**(i) Information security audits/ review**

Binomial test using SPSS was used to evaluate whether there exists any relationship between information security audits/reviews and effective information security management system. One question was asked in relation to this factor.

***Question: Does your institution perform IT security audits/ reviews and vulnerability assessments on a regular basis?***

This question investigates whether public universities carry out information security audits/

reviews regularly.

***Hypothesis testing***

The null and alternative hypotheses are as follows:

Null hypothesis, $H_0$: P = 0.2

Alternative hypothesis, $H_1$: P > 0.2

Where P means proportion of security professionals who indicate their institution has implemented information security audits/reviews.

**Table 19: Binomial Test of information security audit/review factor**

| | | Category | N | Observed Prop. | Test Prop. | Exact Sig. (1-tailed) |
|---|---|---|---|---|---|---|
| Does your institution perform IT security audits/review | Group 1 | Annually | 3 | .5 | .2 | .099 |
| | Group 2 | Don't Audit | 3 | .5 | | |
| | Total | | 6 | 1.0 | | |

The p-value (0.099) is less than 0.1 but greater than 0.05 meaning there is weak evidence in favour of the alternative hypothesis that the proportion of security professionals who indicate their institution performs annual information security audits/reviews is greater than 20%, concluding that there is a relationship between information security audits/reviews and effective ISMS although the relationship is a weak one according to security professionals.

### (j) Physical and environmental security

Binomial test using SPSS was used to evaluate whether there exists any relationship between physical and environmental security and effective information security management system. Two questions were asked in relation to this factor but there was one major question.

***Question: Has physical protection against damage from fire, flood, earthquake, explosion, student unrest, and other forms of natural or man-made disaster been designed and applied?***

This question investigates whether public universities have implemented appropriate physical and environmental controls.

**Hypothesis testing**

The null and alternative hypotheses are as follows:

Null hypothesis, $H_0$: P = 0.2

Alternative hypothesis, $H_1$: P > 0.2

Where P means proportion of security professionals who indicate that their institution has implemented protection against disasters such as fire, floods, earthquake, explosion and student unrest. These are controls in relation to physical and environmental security.

**Table 20: Binomial test of physical and environmental security factor**

| | | Category | N | Observed Prop. | Test Prop. | Exact Sig. (1-tailed) |
|---|---|---|---|---|---|---|
| Is there protection against damage from fire, flood, earthquake, explosion, student unrest | Group 1 | Yes | 5 | .8 | .2 | .002 |
| | Group 2 | No | 1 | .2 | | |
| | Total | | 6 | 1.0 | | |

The significance (p) value of .002 is less than 0.05 therefore the researcher should reject the null hypothesis, concluding that there is a relationship between physical and environmental security and effective ISMS.

**(k) Human resources security**

Binomial test using SPSS was used to evaluate whether there exists any relationship between human resources security and effective information security management system. Two questions were asked in relation to this factor but there was one major question.

***Question: Are security roles and responsibilities clearly stated in your institution's terms and conditions of employment?***

This question investigates whether security roles and responsibilities are addressed in employment and to evaluate whether security professionals consider human resources security a significant factor towards achieving effective ISMS.

**Hypothesis testing**

The null and alternative hypotheses are as follows:

Null hypothesis, $H_0$: P = 0.2

Alternative hypothesis, $H_1$: P > 0.2

Where P means proportion of security professionals who indicate their institution ensures that security roles and responsibilities are included in terms and conditions of employment. This is a control in relation to human resources security.

**Table 21: Binomial Test of human resource security factor**

| | | Category | N | Observed Prop. | Test Prop. | Exact Sig. (1-tailed) |
|---|---|---|---|---|---|---|
| Are security roles and responsibilities includes in terms and conditions of employment | Group 1 | Yes | 5 | .8 | .2 | .002 |
| | Group 2 | No | 1 | .2 | | |
| | Total | | 6 | 1.0 | | |

The significance (p) value of .002 is less than 0.05 and therefore the researcher should reject the null hypothesis, concluding that there is a relationship between human resources security and effective ISMS.

### (l) Cryptography

Binomial test using SPSS was used to evaluate whether there exists any relationship between cryptography and effective information security management system. One question was asked in relation to this factor.

***Question: has your institution implemented encryption?***

This question investigates whether cryptography has been implemented and to evaluate whether security professionals consider cryptography a significant factor towards achieving effective ISMS.

**Hypothesis testing**

The null and alternative hypotheses are as follows:

Null hypothesis, $H_0$: P = 0.2

Alternative hypothesis, $H_1$: P > 0.2

Where P means proportion of security professionals who indicate their institution has implemented encryption

**Table 22: Binomial Test of cryptography factor**

| | | Category | N | Observed Prop. | Test Prop. | Exact Sig. (1-tailed) |
|---|---|---|---|---|---|---|
| My institution uses encryption | Group 1 | Yes | 3 | .5 | .2 | .099 |
| | Group 2 | No | 3 | .5 | | |
| | Total | | 6 | 1.0 | | |

The p-value (0.099) is less than 0.1 but greater than 0.05 meaning there is weak evidence in favour of the alternative hypothesis that the proportion of security professionals who indicate their institution performs regular information security audits/reviews is greater than 20%, concluding that there is a relationship between cryptography and effective ISMS although the relationship is a weak one according to security professionals.

**(m) Hardware and software maintenance (maintain)**

When respondents were asked what procedures they had put in place to update hardware and software, one security professional indicated that they carry out manual updates. This is an indication that security professionals in public universities treated this as an insignificant factor towards the achievement of effective ISMS.

**(n) Communications and operations management**

**Control against malicious code:** When security professionals were asked whether they had virus protection on their machines, it was clear protection against malicious code is a priority in all the public universities. All respondents indicated that they had protection against malicious code. This is an indication that security professionals in public universities treat protection against malicious code as a significant factor towards the achievement of effective ISMS.

**Electronic messaging security:** Majority of security professionals (50%) indicated that their institutions have implemented electronic messaging security as shown in figure 19.

**(o) Management support**

Binomial test using SPSS was used to evaluate whether there exists any relationship between management support and effective information security management system. One question was

asked in relation to this factor.

***Question: Do you consider management support a major IT security barrier in your institution?***

This question investigates whether management support is an important factor in towards achieving effective ISMS.

**Hypothesis testing**

The null and alternative hypotheses are as follows:

Null hypothesis, $H_0$: P = 0.2

Alternative hypothesis, $H_1$: P > 0.2

Where P means proportion of security professionals who indicate that management support is ***not*** a major barrier to IT security in their institution.

**Table 23: Binomial Test of management support factor**

| | | Category | N | Observed Prop. | Test Prop. | Exact Sig. (1-tailed) |
|---|---|---|---|---|---|---|
| Major barrier to IT security is lack of senior management support | Group 1 | No | 4 | .7 | .2 | .017 |
| | Group 2 | Yes | 2 | .3 | | |
| | Total | | 6 | 1.0 | | |

The significance (p) value of .017 is less than 0.05 therefore the researcher should reject the null hypothesis, concluding that there is a relationship between management support and effective ISMS.

## 4.5 Summary of statistical analysis of the factors influencing the overall effectiveness of an information security management system.

Survey results indicate a number of factors influence the overall effectiveness of an information security management system. Based on this study information security policy, incident response capability, communications and operations security and human resources security are the most important information security factors. Based on refined ISM factors as well as the analysis of relationships between effective ISM and various ISM factors, a refined framework for information security management in public universities is illustrated in the table 24.

Security professionals have indicated that risk assessment is not an important factor in information security management. This deserves serious attention because effective information security can only be achieved if an organization knows the risks to its information assets.

**Table 24: Summary of Factors that influence the overall effectiveness of an information security management system according to security professionals.**

| Category (Broad Factors) | Specific Factors | P -Value | Nature of influence |
|---|---|---|---|
| ISMS Planning | Security policy | 0.002 | Major factor |
| | Management support | 0.017 | Important factor |
| Implementation and operation of controls | Incident response | 0.002 | Major factor |
| | Communications and operations security | | Major factor |
| | Physical and environmental security | 0.002 | Major factor |
| | Human resources security | 0.002 | Major factor |
| | Access control | 0.099 | Weak factor |
| | Contingency planning | 0.017 | Important factor |
| | cryptography | 0.099 | Weak factor |
| | Asset classification and control | 0.002 | Major factor |
| Awareness, training and education | Information security awareness | 0.002 | Major factor |
| Review/ Audit | Information security audits/ reviews | 0.099 | Weak factor |

## 4.6 DISCUSSION

It is vital that public universities in Kenya put appropriate controls in place to secure information assets. The main objective of this study was to investigate information security management systems in public Universities in Kenya as. Based on the findings of this research, it is evident that public Universities in Kenya are responding to information security threats using a variety of security technologies as shown in figure 9. The survey findings however indicate that the information security control environment is inadequate to deal effectively with information security threats. Most security professionals (100%) indicated that their institutions had an information security policy. The results of this study however show that risk assessment was not used as the basis for formulating information security policy as well as the selection of information security controls as shown in figure 7. Proper information security is only possible on the basis of sound risk analysis.

Good security also calls for a balance between technological and human behavioral controls. For example, an institution with outstanding technical controls may still experience security issues because people intentionally and unintentionally violate IT security policies. Furthermore, technical safeguards may be compromised when a user discloses his or her password, sends out confidential information in an e-mail or clicks on a malicious link or e-mail attachment. This therefore means that human factor in information security cannot be under-estimated. Surprisingly, only 21.7% of the users indicated that a formal information security awareness program for staff existed in their institutions as shown in figure 14. In addition, only 16% of the users had received training on information security (Figure 15). A robust information security awareness and training program is an essential element of an effective information security management system. People should be aware of their security roles and responsibilities. Without proper security awareness training, users may not be aware of security risks and how these risks may be overcome within their day-to-day job functions.

Key literature in information security management suggests that organizations are in a better position to deal effectively with information security incidents if they have implemented information security incident reporting and management procedures. The study findings show that a majority of the institutions were ill prepared to deal with information security incidents as shown in figure 13. There is widespread lack of any formal procedures for information security

incident management. Majority of the users (72%) indicated that their institutions had not implemented incident reporting and management procedures. This means that it may be very difficult to react quickly and efficiently to disruptions of services.

The survey results also show that most institutions had a process in place to ensure selection of strong passwords according to most security professionals (50%) as shown in figure 10. The study however shows that there is lack of understanding among some users in the public universities about what constitutes a good password, meaning that password policies were not communicated and enforced in some of the institutions. When asked what best describes a good password, majority of the users (96%) indicated that a good password is one that includes upper and lower case letters, numbers and special characters as shown in figure 11. However, 48% of the users preferred using a password they can remember such as their name. Such a password would be easy to guess and it does not conform to best practices in password selection. Furthermore, when asked when they last changed their passwords, it emerged that 12% of the users had never changed their passwords as shown in figure 12. Poor password selection is frequently a major problem for any system's security. A password is a critical line of defense and therefore good security practices in the selection of passwords will keep information secure.

Contingency planning was identified as a critical success factor towards achieving an effective information security management system (figure 6). This study reveals that in most of the public universities, contingency planning has not been adequately addressed to ensure that business processes can be restored in a timely manner after disruptions. Major components of a contingency plan include an Incident response plan, Business continuity plan and Disaster recovery plan. According to the survey, only 33.3% of the security professionals indicated that their universities had implemented a DRP as shown in figure 8. In addition, majority of the security professionals (83.3%) indicated that their institutions had not implemented an IRP. None of the institutions has implemented a Business continuity plan.

Based on the research findings also, a majority of the public universities have not addressed the security-related risks associated with employees, vendors and suppliers. The security professionals in the public universities indicated that employees/contractors who have privileged access to information systems had not undergone background security investigations.

Furthermore, 83.3% of information systems users indicated that security roles and responsibilities were not included in the terms and conditions of employment. During employment, Public universities should ensure that all employees, contractors and third party users are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support organizational security policy in the course of their normal work, and to reduce the risk of human error.

Key literature suggests that information security audits/reviews form an important part of any successful information security management system. This study has revealed that some public universities don't carry out information security audits/reviews. Fifty percent (50%) of the security professionals indicated that their institutions don't carry out information security audits/ reviews as shown in figure 21. Information security audits are intended to improve the level of information security, avoid improper information security designs, and optimize the efficiency of the security safeguards and security processes.

Survey results have also shown that termination of access rights for employees whenever their employment is terminated has not been adequately addressed. A remarkable percentage (66.7%) of security professionals indicated that access rights are not usually terminated upon termination of employment.

The success of any information security initiative also depends on among other factors consistent commitment by top management and the associated outcomes including approval of IT security decisions and allocation of necessary resources. Based on the findings of this research, enforcement of policies, lack of senior management support and lack of resources were cited as the major barriers to IT security according a majority of the security professionals as shown in figure 20. Security is not free and therefore public universities should be prepared to spend more on information security to safeguard their information technology assets.

As regards security of electronic messaging, majority (50%) of security professionals indicated that their institution has implemented security for electronic messaging however the measures put in place in some public universities were seriously inadequate. Some public universities is only using a firewall. This means that incoming and outgoing mail is never scanned for

malicious content. Most of security professionals mentioned controls such as firewalls (50%) while others mentioned encryption and passwords (25%) as shown in table 9.

The general perception of most users is that their institutions have not done enough to protect information systems. Survey results indicate that a clear majority of respondents believe that their institutions have not done enough to protect information systems. Furthermore, approximately 50% of the users indicated that their institutions had suffered a security breach in the last two years as shown in figure 23. Some of the security breaches were internal others external.

This study also sought to determine whether there exist any relationship between the dependent variable and the independent variables. It emerged that there is a relationship between dependent variable (effective ISMS) and independent variables. Furthermore, information security policy, incident response capability, communications and operations security and human resources security are the most important information security factors.

# CHAPTER FIVE

# CONCLUSIONS AND RECOMMENDATIONS

## 5.1 SUMMARY OF CONTRIBUTIONS/ ACHIEVEMENTS

This research work has made several contributions towards the achievement of the intended objectives. It is of significant value to public universities in Kenya in as far as information security management is concerned.

The factors that determine the overall effectiveness of an information security management system were identified through the analysis of the current key literature on this topic of information security management (ISO 27001 Standard & NIST Special Publications). Information security practitioners facing this challenge will find this relevant and important since these are the critical success factors towards the implementation of a successful information security program.

This study has also contributed to the domain of information security management by developing a framework for information security management grounded on internationally recognized best practice guidelines and recommendations in information security management. The framework can be used as a blueprint against which universities attempting to implement effective information security management system can use to benchmark their practices.

This research has also provided insightful information regarding information security controls and related information security management practices in public universities in Kenya. Additionally main issues, barriers and factors that influence information security management in public universities in Kenya have been highlighted with recommendations about how to address them to secure information assets.

## 5.2 LIMITATIONS OF THE STUDY

This study was carried out in public universities in Kenya. Due to budget and time constraints, the researcher could not carry out the study in all public universities. Being an outsider also, there are bound to be some aspects of leadership practice and organizational culture that may not have been revealed during the study.

Another limitation is that the study focused much on key issues and factors influencing information security management in public universities in Kenya. The study did not however look at security related to information systems acquisition and development which is also an important consideration in effective information security management. Most public universities are embracing open standards

In addition, the research did not consider legal and regulatory compliance aspects. This is because there is no explicit legislation on information security management in public universities in Kenya.

## 5.3 CONCLUSIONS

The main aim of this research was to investigate current information security management practices in Kenyan public universities to establish whether they conform to industry best practices in information security management. In this respect, a framework for information security management grounded on internationally recognized best practice guidelines and recommendations in information security management was developed which guided a comprehensive study to understand the status of information security control environment in these institutions. The dependent variable for this study was effective ISMS and the independent variables were ISM best practices identified through analysis of key literature in information security management (ISO 27001 and NIST Special Publications). The proposed framework can be used as a blueprint against which universities attempting to implement effective information security management system can use to benchmark their ISM practices.

Another goal of this study was to determine whether there exist gaps between common information security management practices in public universities in Kenya and industry best practices. The study has provided insightful information regarding information security controls implemented and related information security management practices. The main issues, barriers and factors that influence information security management in public universities in Kenya have been highlighted with recommendation of how to address them to secure information assets.

The study findings indicate that the information security control environment in public universities is inadequate to deal effectively with information security threats. A majority of the

public universities are ill prepared to deal with information security incidents as shown in figure 13. Furthermore, contingency planning has not been adequately addressed to ensure that business processes can be restored in a timely manner after disruptions as shown in figure 8. The main barriers to information security include enforcement of policies, lack of senior management support and lack of resources.

## 5.4 RECOMMENDATIONS

Public Universities in Kenya should adopt the proposed framework for information security management to effectively manage the security of information. This research has established that there are several gaps/deficiencies in the security management practices adopted in public universities. To improve information security in public universities, the study recommends the following.

**Risk Assessment:** Proper information security is only possible on the basis of sound risk analysis. Public Universities should therefore use risk analysis as the basis for formulation of information security policy as well as selecting information security controls.

**Policy and enforcement:** Information security policy should be implemented and enforced to keep information secure. Password policies should be implemented and enforced to ensure the selection of strong passwords. The results of this study reveal that some users use weak passwords. Poor password selection is frequently a major problem for any system's security. Practically it can be challenging to ensure that staff and students have read, understood and complied with policies but the policies cannot be effective unless they are widely understood and enforced.

**Management approval and support:** Management should ensure that proper resources are available and that all employees affected by the ISMS have the proper training, awareness and competency. Security is not free and therefore top management in public universities must be willing to spend a little more to safeguard their information assets. Enforcement of policies, lack of resources and lack of management support were cited as the major barriers to IT security according a majority of the respondents as shown in figure 20. Management needs to realize the value of information security in their institutions. Furthermore, security professionals must increase communication with management and increase information security awareness

appropriately within the organization as well as propose applicable solutions.

**Information Security awareness and education programs:** Education and awareness programs may be the single most effective way to sensitize staff and students about their security roles and responsibilities. If staff and students don't know what they are supposed to be doing they will most likely not do it. Lack of awareness is one of the leading barriers to information security in public universities.

**Contingency planning:** Public universities should appropriately plan for contingencies (contingency planning) to enable them to effectively react to and recover from events that threaten the security of information and information technology assets. Major components of a good contingency plan would include an Incident response plan, Business continuity plan and Disaster recovery plan.

**Human Resource security:** During employment, Public universities should ensure that all employees, contractors and third party users are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support organizational security policy in the course of their normal work, and to reduce the risk of human error. Security-related risks associated with vendors and suppliers should also be thoroughly addressed.

**Incident Reporting and Management:** The widespread lack of formal procedures for information security incident management is a clear demonstration of ineffective information security programs. An incident-handling capability can provide the ability to react quickly and efficiently to disruptions of services. Therefore public universities in Kenya should implement appropriate incident handling procedures to effectively deal with information security incidents whenever they occur.

**Information security audits/reviews*:*** Information security audits/reviews form an important part of any successful information security management system. Public universities must therefore periodically carry out information security audits/ reviews to improve the level of information security and optimize the efficiency of security safeguards and processes.

## 5.5 SUGGESTIONS FOR FURTHER WORK/ RESEARCH

Due to time constraints, the researcher could not undertake extensive work/research to ascertain adequacy of security policy to address information security. Information security policy is the cornerstone of information security and therefore unless it is well formulated, communicated and enforced, it is not possible to achieve information security management objectives. The researcher therefore recommends further research to get insightful information regarding information security policy structure and content in these institutions and to determine whether they are adequate enough to address information security issues.

In addition, the proposed framework for information security management in public universities can be further refined by further streamlining/refining the information security management practices that determine the effectiveness of an information security management system. This can be done by studying what most certified information security professionals are doing to achieve ISM objectives in both public and private sector. The most prevalent practices from the survey data can then be used to refine the framework to come up with an ISMS framework that is applicable across most organizations.

## REFERENCES


Arnason, S.T. and Willet, K.D. (2008). *How to Achieve 27001 Certification: An Example of Applied Compliance Management.* New York: Auerbach Publications.

Bishop, M. (2004). *Introduction to Computer Security*. Prentice Hall PTR.

Calder, A. and Watkins, S. (2008). *IT Governance: A Manager's guide to Data Security and ISO27001/ISO 27002, 4th Edition*. London: Kogan Page Limited.

Dawson, C. (2002). *Practical Research Methods: A user friendly guide to mastering research.* Oxford: How To Books Ltd.

Federal Financial Institutions Examination Council (2006). *Information security IT Examination Handbook.*

Harold, F. T. ed. (2010). *Official (ISC)² Guide to the CISSP CBK, 2nd Edition.* New York: Auerbach Publications.

Kimwele, M., Mwangi, W. and Kimani, S. (2011). *Information Technology (IT) Security Framework for Kenyan Small and Medium Enterprises (SMEs)*. International Journal of Computer Science and Security (IJCSS), Volume (5): Issue (1): 2011

Kothari, C.R. (2004). *Research Methodology- Methods and Techniques, 2nd Revised Edition*. New Delhi: New Age International (P) Limited Publishers.

Maiwald, E. (2001). *Network Security: A Beginner's guide*. Newyork: The McGraw-Hill Companies, Inc.

Marczyk, G., DeMatteo, D. and Festinger, D. (2005). *Essentials of Research Design and Methodology.* New Jersey: John Wiley & Sons, Inc.

Mugenda and Mugenda .(2008). Research Methodology; First Edition, Longman publishers

National Security Agency, USA. (2002). *The 60 Minute Network Security Guide (First Steps Towards a Secure Network Environment).*

Peltier, T.R., Peltier J., and Blackley J. (2005). *Information security fundamentals*.CRC Press.

Peltier, T.R. (1999). *Information Security Policies and Procedures: A Practitioner's Reference.* New York: Auerbach Publications.

Saltzer, J. and M. Schroeder, M. (1975). "The Protection of Information in Computer Systems," Proceedings of the IEEE 63 (9), pp. 12781308 (Sep. 1975).

Stewart, J. M., Tittel, E. and Chapple, M. (2008). *CISSP: Certified Information Systems Security Professional StudyGuide, 4th Edition.* Indiana: Wiley Publishing, Inc

Tipton, Harold F. and Micki K. eds (2000). *Information Security Management Handbook, 4th Edition*. New York: Auerbach Publications.

## INTERNET SOURCES

Bassham, Lawrence E., and W. Timothy Polk. *Threat Assessment of Malicious Code and Human Threats.* National Institute of Standards and Technology Computer Security Division. http://csrc.nist.gov/publications/nistir/threats/threats.html

Bragg, B. (2011). *Common ISO 27001 Gaps* [online]. Available at: http://www.dionach.com/pdf/Common-ISO-27001-Gaps-ISSA0111.pdf [Accessed 11 June 2012]

CIO East Africa (2012). *103 Government of Kenya websites hacked overnight* [online]. Available at: http://www.cio.co.ke/news/main-stories/103-Government-of-Kenya-websites-hacked-overnight/**.** [Accessed 11 June 2012]

Commission of Higher Education (2012). *Status of Universities in Kenya* [online]. Available at: http://www.che.or.ke/status.html. [Accessed 11 July 2012]

Deloitte East Africa (2011). *2011 East Africa Application Security Survey, safeguarding the future* [online]. Available at: http://www.deloitte.com/view/en_KE/ke/eamedia/kepublications/surveyreports/index.htm. [Accessed 10 July 2012]

Educause Center for Applied Research (2003). *Information Technology Security: Governance, Strategy and Practice in Higher Education* [online], Volume 5. Available at: http://net.educause.edu/ir/library/pdf/ers0305/rs/ers0305w.pdf. [Accessed 12 July 2012]

Educause Center for Applied Research (2006). *Campus IT Security: Governance, Strategy, Policy, and Enforcement* [online], Volume 2006, Issue 17. Available at: http://net.educause.edu/ir/library/pdf/ERB0617.pdf. [Accessed 13 July 2012]

IBM. *IBM Security: Security Intelligence – Think Integrated*. Available at: http://www-142.ibm.com/software/products/us/en/category/SWI00 [Accessed 11 June 2012]

Information Systems Audit and Control Association. *COBIT 4.1 Excerpt* [online]. Available at: http://www.isaca.org/Knowledge-Center/cobit/Documents/COBIT4.pdf [Accessed 10 July 2012]

ISO27k Forum (2011). *The Free ISO27k Toolkit: ISO/IEC 27001 Gap Analysis and Statement of Applicability* [online]. Available at: http://www.iso27001security.com/html/iso27k_toolkit.html [Accessed 10 July 2012]

Ministry of Education (2007). *Press Release By Hon. Minister For Education - Friday, 25th May 2007 on the eve of "2nd International Conference on ICT for Development , Education and Training - E-Learning Africa* [online]. Available at: http://www.elearning-africa.com/pdf/press/press_kit/Kenyan_Ministry_of_Education.pdf. [Accessed 11 June 2012]

National Institute of Standards and Technology (1995). *An Introduction to Computer Security:*

*The NIST Handbook, Special Publication 800-12* [online] Available at: http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf. [Accessed 23 July 2012]

National Institute of Standards and Technology (2003). *Guide to Information Technology Security Services, Special Publication 800-35* [online] Available at: http://csrc.nist.gov/publications/nistpubs/800-35/NIST-SP800-35.pdf. [Accessed 23 July 2012]

National Institute of Standards and Technology (2003). *Building an Information Technology Security Awareness and Training Program, Special Publication 800-50* [online] Available at: http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf [Accessed 13 June 2012]

National Institute of Standards and Technology (2007). *Information Security – Recommended information security controls for federal information systems, Special Publication 800-53, Revision 3* [online] Available at: http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf [Accessed 23 July 2012]

National Institute of Standards and Technology (2010). *Contingency Planning Guide for Information Technology Systems, Special Publication 800-34 Rev.1* [online] Available at: http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf. [Accessed 13 June 2012]

National Institute of Standards and Technology (2007). *Guide to Secure Web Services, Special Publication 800-95* [online] Available at: http://csrc.nist.gov/publications/nistpubs/800-95/SP800-95.pdf. [Accessed 13 June 2012]

National Institute of Standards and Technology (2002). *Risk Management guide for information technology systems, Special Publication 800-30* [online] Available at: http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf. [Accessed 23 July 2012]

National Institute of Standards and Technology (2007). *Guidelines for securing electronic messaging, Special Publication 800-45v2* [online] Available at: http://csrc.nist.gov/publications/nistpubs/800-45-version2/SP800- 45v2.pdf [Accessed 23 July 2012]

National Institute of Standards and Technology (2002). *Information Technology Security Training Requirements: A Role-and Performance-Based Model, Special Publication 800-16* [online] Available at: http://csrc.nist.gov/publications/nistpubs/800-16/sp800-16.pdf. [Accessed 23 July 2012]

Sante, T.S. and Ermers, J. (2009).*The IT Management Group TOGAF 9 and ITIL V3: Two frameworks white paper* [online]. Available at: http://www.togaf.biz/TOGAFWebsitefiles/TOGAF%209%20and%20ITIL%20V3.pdf. [Accessed 11 July 2012]

The Star (2011). *Student fails to stop KU graduation date* [online] Available at: http://www.the-star.co.ke/national/national/52785-student-fails-to-stop-ku-graduation-date (Accessed: 13 June 2012)

United States Department of Agriculture (2011). *FY2012 Information Security Awareness* [online]. Available at: http://www.wi.nrcs.usda.gov/about/FY12InformationSecurityAwarenessPaper.pdf [Accessed 10 July 2012]

Wanjiku, R. (2008) *Kenya works on training information security managers* [online]. Available at: http://www.computerworld.com/s/article/9080919/Kenya_works_on_training_information_security_managers. [Accessed 12 July 2012]

## APPENDIX A: LETTER OF INTRODUCTION

Dear Sir/Madam,

My name is Philip M. Kitheka, a student pursuing MSc. Information systems at the University of Nairobi. I am undertaking a research study entitled " Information security management in public universities in Kenya: A gap analysis between common practices and industry best practices". I would be grateful if you would volunteer to assist in this project by completing the attached questionnaire.

The research study is designed to investigate information security management systems in public universities in Kenya and to determine and analyze the gaps between actual information security controls and related security management practices, and industry best practices in information security management. Participation in the study involves completion of a questionnaire which consists of 2 parts and which may require approximately 15 to 25 minutes to complete.

The study will cover information security controls, information security management systems, information security policy, Organization of information security, Asset management, human resources security, physical and environmental security, operations security, information systems acquisition, development & maintenance, Incident management, Business continuity management and compliance to regulatory and legal framework.

Please complete the survey by January 10, 2013. I appreciate your time and candor. The survey does not need to be completed at a single sitting. You can save your responses and return to it at times that are convenient for you. You may also wish to consult with colleagues about answers to particular questions, or if another person in your institution is better positioned to answer this survey, please forward this e-mail to that person.

Be assured that any information provided will be treated in the strictest confidence and none of the participants will be individually identifiable in the resulting thesis, report or other publications. You are, of course also, entirely free to discontinue your participation at any time or to decline to answer particular questions. Any enquiries you may have concerning this research study should be directed to me by email (kithekap@hotmail.com)

Thank you for your attention and assistance.

**Yours sincerely,**

**Philip M. Kitheka**

## APPENDIX B: INFORMATION SECURITY MANAGEMENT QUESTIONNAIRE (SECURITY PROFESSIONALS)

My name is Philip M. Kitheka, a student pursuing M.Sc. Information systems at the University of Nairobi. I am undertaking a research study entitled " Information security management in public universities in Kenya: A gap analysis between common practices and industry best practices". I would be grateful if you would volunteer to assist in this project by completing this questionnaire. Please complete the questionnaire by January 20, 2013

### 1.0 GENERAL INFORMATION

1.1 Survey ID: _____

1.2 Your Institution: _____

1.3 How many staff does your institution employ? _____

1.4 Has your institution ever been compromised in the last 2 years? ☐ Yes ☐ No ☐ Don't Know

1.5 If yes, was the institution compromised internally, externally or both? ☐ Internally ☐ Externally ☐ Both

### 2.0 INFORMATION SECURITY CONTROLS AND RELATED SECURITY MANAGEMENT PRACTICES

2.1 What is the title of the position with day-to-day management responsibility for IT Security?

_____

2.2 What Security Qualification/ Certification does the person hold?

☐ CISSP ☐ CISA/CISM ☐ GIAC ☐ SSCP ☐ Security+ ☐ None ☐ Other (Specify):

_____

2.3 Have you received any training in information security? ☐ Yes ☐ No

2.4 My institution has a formal IT Security awareness program for it's

Students: ☐ Yes ☐ No ☐ Don't Know

Employees: ☐ Yes ☐ No ☐ Don't Know

2.5 Does your institution have an information security policy? ☐ Yes ☐ No ☐ Don't Know

2.6 Select what exactly describes your information security policy

Information security policy has been approved by top management (Vice Chancellor)
☐ Yes ☐ No ☐ Don't Know

Information security policy has been communicated to all employees and relevant external parties ☐ Yes ☐ No ☐ Don't Know

Violation of information security policy is punishable ☐ Yes ☐ No ☐ Don't Know

Information Security Policy is published/ Available online through our website
☐ Yes ☐ No ☐ Don't Know

I have read and understood my institution information security policy
☐ Yes ☐ No ☐ Don't Know

2.7 Does your institution provide remote network access? ☐ Yes ☐ No ☐ Don't Know

2.8 Are all assets clearly identified and an inventory of all important assets drawn up and maintained? ☐ Yes ☐ No ☐ Don't Know

2.9 Describe your institution's current approaches to IT Security (Select appropriately)

(i) Network firewall ☐ Yes ☐ No ☐ Don't Know

(ii) Intrusion Detection system (IDS) ☐ Yes ☐ No ☐ Don't Know

(iii) Intrusion Prevention System (IPS) ☐ Yes ☐ No ☐ Don't Know

(iv) VPN for remote access ☐ Yes ☐ No ☐ Don't Know

(v) Secure sockets layer (SSL) for secure Web transactions ☐ Yes ☐ No ☐ Don't Know

(vi) Integrated threat management (ITM) ☐ Yes ☐ No ☐ Don't Know

(vii) Centralized backup system ☐ Yes ☐ No ☐ Don't Know

(viii) Encryption ☐ Yes ☐ No ☐ Don't Know

(ix) Active content monitoring/ filtering ☐ Yes ☐ No ☐ Don't Know

(x) Other (Specify): _____

2.10 Has your institution undertaken a risk assessment to determine the value of your IT assets and risk to those assets? ☐ Yes ☐ No ☐ Don't Know

2.11 Does your institution have an ISMS Policy? ☐ Yes ☐ No ☐ Don't Know

2.12 Have employees and/or contractors who have privileged access to IT systems undergone background investigations? ☐ Yes ☐ No ☐ Don't Know

2.13 Does your institution perform IT security audits/ reviews and vulnerability assessments on a regular basis? Select. ☐ Monthly ☐ Quarterly ☐ Annually ☐ Don't Audit

☐ Other (Specify)

2.14 Do you have a formal IT security incident handling procedure? ☐ Yes ☐ No

Briefly describe the procedure:

2.15 What are the major barriers to IT security at your institution (Select all that apply)

☐ Enforcement of policies ☐ Technology ☐ Awareness ☐ Senior Management support

☐ Resources ☐ Absence of policies

2.16 Have plans been developed and implemented to maintain or restore operations and ensure availability of information at the required level and in the required time scales following interruption to, or failure of, critical business processes? ☐ Yes ☐ No ☐ Don't Know

2.17 Is your institution prepared for unexpected events? (Make Appropriate Selection)

My institution has implemented an incident response plan (IRP) ☐ Yes ☐ No

My institution has implemented a disaster recovery plan (DRP) ☐ Yes ☐ No

My institution has implemented a business continuity plan (BCP) ☐ Yes ☐ No

2.18 Is there a formal user registration and de-registration procedure in place for granting and revoking access to all information systems and services? ☐ Yes ☐ No

2.19 How often do you do back-ups?

2.20 Has physical security for offices, rooms, and facilities been designed and applied?

☐ Yes ☐ No ☐ Don't Know

State physical controls implemented and where.

2.21 Has physical protection against damage from fire, flood, earthquake, explosion, student unrest, and other forms of natural or man-made disaster been designed and applied?

☐ Yes ☐ No ☐ Don't Know

Briefly describe the controls in Place

2.22 Do you have virus protection installed? ☐ Yes ☐ No ☐ Don't Know

2.23 How often is it updated and is it automatic?

2.24 What procedures have been implemented to update software and hardware

2.25 Are security roles and responsibilities clearly stated in your institution's terms and conditions of employment? ☐ Yes ☐ No

2.26 Upon termination of a person's employment, does your institution make sure that the person has returned the institution's information assets in his (or her) possession and then remove his (or her) access right in an appropriate manner? ☐ Yes ☐ No

2.27 Do you think in your opinion your institution has done enough to protect information systems? ☐ Yes ☐ No

2.28 Is there a process in place that ensures users follow good security practices in the selection and use of passwords? ☐ Yes ☐ No

2.29 What best describes a good password?

(i) It is what I can remember like my name ☐ Yes ☐ No

(ii) Includes upper and lower case letters, numbers, and special characters ☐ Yes ☐ No

(iii) Should not be complex ☐ Yes ☐ No

(iv) Don't Know ☐ Yes ☐ No

2.30 When did you last change your password?

☐ 1 Month ☐ 4 Months ☐ 6 Months ☐ 1 Year ☐ 2 Years ☐ 3 Years

☐ Other (Specify)

2.31 Why did you change your password?

2.32 Is information involved in electronic messaging appropriately protected? What security measures are in place?

2.33 Does your institution check the operational status of the implemented security measures, such as by recording and maintaining access logs, checking for unauthorized operations to the important information? ☐ Yes ☐ No

## APPENDIX C: RECOGNIZED PUBLIC UNIVERSITIES IN KENYA

**Source: Commission for University Education**

1. University of Nairobi (UoN)
2. Moi University (MU)
3. Kenyatta University (KU)
4. Egerton University (EU)
5. Jomo Kenyatta University of Agriculture and Technology (JKUAT)
6. Maseno University (MSU)
7. Masinde Muliro University of Science and Technology (MMUST)
8. Dedan Kimathi University of Technology (DKUT)
9. Chuka University (CU)
10. Technical University of Kenya (TUK)
11. Technical University of Mombasa (TUM)
12. Pwani University (PU)
13. Kisii University (EU)
14. University of Eldoret
15. Maasai Mara University
16. Jaramogi Oginga Odinga University of Science and Technology
17. Laikipia University
18. South Eastern Kenya University
19. Meru University of Science and Technology
20. Multimedia University of Kenya
21. University of Kabianga
22. Karatina University

## APPENDIX D: INFORMATION SECURITY MANAGEMENT QUESTINNAIRE (END USERS)

My name is Philip M. Kitheka, a student pursuing M.Sc. Information systems at the University of Nairobi. I am undertaking a research study entitled " Information security management in public universities in Kenya: A gap analysis between common practices and industry best practices". I would like to ask you some questions regarding information security practices in your institution. I would be grateful if you would volunteer to assist.

### 3.0 GENERAL INFORMATION

3.1 Survey ID: _____

3.2 Your Institution: _____

3.3 Has your institution ever been compromised in the last 2 years? ☐ Yes ☐ No ☐ Don't Know

3.4 If yes, was the institution compromised internally, externally or both? ☐ Internally ☐ Externally ☐ Both

3.5 What is your occupation? _____

### 4.0 INFORMATION SECURITY CONTROLS AND RELATED SECURITY MANAGEMENT PRACTICES

4.1 Have you received any training in information security? ☐ Yes ☐ No

4.2 My institution has a formal IT Security awareness program for it's

Students: ☐ Yes ☐ No ☐ Don't Know

Employees: ☐ Yes ☐ No ☐ Don't Know

4.3 Does your institution have an information security policy? ☐ Yes ☐ No ☐ Don't Know

4.4 Select what exactly describes your information security policy

Information security policy has been approved by top management (Vice Chancellor)

☐ Yes ☐ No ☐ Don't Know

Information security policy has been communicated to all employees and relevant external parties ☐ Yes ☐ No ☐ Don't Know

Violation of information security policy is punishable ☐ Yes ☐ No ☐ Don't Know

Information Security Policy is published/ Available online through our website

☐ Yes ☐ No ☐ Don't Know

I have read and understood my institution information security policy

☐ Yes ☐ No ☐ Don't Know

4.5 Do you have virus protection installed? ☐ Yes ☐ No ☐ Don't Know

4.6 If yes, is it open source (free) antivirus software or is it a commercial antivirus? (State the type/ Vendor)

4.7 Do you have a formal IT security incident handling procedure in your institution? ☐ Yes ☐ No

Briefly describe the procedure:

4.8 Has physical security for offices, rooms, and facilities been designed and applied?

☐ Yes ☐ No ☐ Don't Know

State physical controls implemented and where.

4.9 Are security roles and responsibilities clearly stated in your institution's terms and conditions of employment? ☐ Yes ☐ No

4.10 Is there a process in place that ensures users follow good security practices in the selection and use of passwords? ☐ Yes ☐ No

4.11 What best describes a good password?

(v) It is what I can remember like my name ☐ Yes ☐ No

(vi) Includes upper and lower case letters, numbers, and special characters ☐ Yes ☐ No

(vii) Should not be complex ☐ Yes ☐ No

(viii) Don't Know ☐ Yes ☐ No

4.12 When did you last change your password?

☐ 1 Month ☐ 4 Months ☐ 6 Months ☐ 1 Year ☐ 2 Years ☐ 3 Years

☐ Other (Specify)

4.13 Why did you change your password?

4.14 Do you think in your opinion your institution has done enough to protect information systems? ☐ Yes ☐ No