UNIVERSITY OF NAIROBI

INSTITUTE OF DIPLOMACY AND INTERNATIONAL STUDIES (IDIS)

THE ROLE OF INFORMATION SECURITY MANAGEMENT SYSTEM IN PROMOTING AFRICAN DEVELOPMENT: A CASE STUDY OF KENYA

GODFREY BUSOLO
ADM. NO. R50/9975/2018

SUPERVISOR: DR. PATRICK MALUKI

A RESEARCH PROJECT SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENT FOR AWARD OF MASTERS OF ARTS DEGREE IN INTERNATIONAL STUDIES AT THE INSTITUTE OF DIPLOMACY AND INTERNATIONAL STUDIES (IDIS), UNIVERSITY OF NAIROBI

SEPTEMBER, 2018

DECLARATION

I declare that this research project is my original work and that it has not been presented for examination purpose in any university or other related institution

Sign……..Date……

Godfrey Busolo

This research project has been submitted for examination with my approval as the university supervisor.

Sign……..Date……

Dr. Patrick Maluki

DEDICATION

This research project is dedicated to all those who provided a constant source of encouragement and support during the study period.

ACKNOWLEDGEMENT

First and foremost, I thank God for the gift of life and for giving me strength to chase my dreams.

I would also like to express my sincere gratitude to my project advisor Dr. Patrick Maluki for his guidance and support throughout this study and for his confidence in me. In addition, I thank the faculty members of both the University of Nairobi's Institute of Diplomacy and International Studies led by Prof. Maria Nzomo and the National Defence College of Kenya under the stewardship of Major General Andrew Ikenye, for the useful insights shared before and during the study. I am also grateful to fellow course participants of NDC 20:2017/2018 for the stimulating discussions, for the many moments of crisis and sleepless nights and for all the fun we had for the duration of the academic programme.

The production of this paper would not have been possible without research data. In this regard, I am indebted to all those who facilitated data collection through both primary and secondary sources. These include the staff of the Ministry of Information, Communication and Technology and the Kenya ICT Authority, some of who participated in Key Informant Interviews.

Finally, I thank my family, friends and the National Treasury fraternity for the moral and material support provided towards the programme.

Thank you and God bless you all.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AUC	-	African Union Commission
BSI	-	British Standards Institution
CCTV	-	Closed-circuit Television
COBIT	-	Control Objectives for Information and related Technology
CNE	-	Computer Network Exploration
IEC	-	International Electro-technical Commission
ISACA	-	Information Systems Audit and Control Association
ISM	-	Information Security Management
ISMS	-	Information Security Management System
ISO	-	International Organization for Standards
ISSM	-	Information Systems Success Model
ICT	-	Information Communication and Technology
IT	-	Information Technology
ITIL	-	Information Technology Infrastructure Library
KE-CIRT	-	Kenya Computer Incident Response Team
MDAs	-	Ministries, Departments and Agencies
MFIs	-	Micro Finance Institutions
NEPAD	-	New Partnership for African Development
OECD	-	Organization for Economic Cooperation and Development
SMEs	-	Small and Medium Enterprises
TVET	-	Technical and Vocational Educational Training
UAV	-	Unmanned Aerial Vehicle
UN	-	United Nations
UNESCO	-	United Nations Educational, Scientific and Cultural Organization

ABSTRACT

The world has over the recent past witnessed numerous cases of unauthorized access to official information. The realities of globalization coupled with the dynamic nature of the 21st century have significantly contributed to this state of affairs thereby making information security an issue of global concern. In this regard, implementation of the Information Security Management System (ISMS) has been highlighted as one possible way through which organizations can secure their information assets. The question, however, is what are the key success factors of ISMS and where does Kenya in particular and Africa in general stand as far as ISMS is concerned? To this end, this study sought to examine key issues and factors influencing implementation of effective ISMS amongst African public sector institutions. It also sought to review Kenya's institutional and policy framework on information security. Lastly, it sought to assess the extent and effect of application of ISMS principles in the Kenya public sector policy environment. In undertaking the study, both primary and secondary sources of data were accessed. Primary data was obtained through observation and key informant interviews with relevant Government officials in respect of the research area. Secondary data was, on the other hand, collected through content analysis of government records, journals, reports and books. The data was thereafter consolidated based on the various ISMS themes.The systems theory of management informed the study from the standpoint that ISMS is a sub-system that contributes to the effective operation of the organizational system through, inter alia, control and protection of information assets. Study findings revealed that ISMS is a business approach to the overall management of an organization that accentuates analysis of security requirements for each information resource and application of appropriate controls to guarantee protection of these assets. The study also established that successful implementation of the system requires commitment from the uppermost level of an organization. Further, it established that there are numerous benefits associated with ISMS and that the system contributes towards the realization of a proficient public sector amongst African states and ultimately national development. Finally, the study established that the Kenyan Government has been pursuing implementation of the principles of ISMS in the public sector through a number of statutes, policies and guidelines and that there exists an elaborate institutional arrangement on information, communication and technology. To ensure effective implementation of government guidelines on ISMS, it is recommended that the Kenya ICT Authority develops an appropriate monitoring and evaluation mechanism to guide in assessing performance of Ministries Departments and Agencies (MDAs). It is also recommended that all MDAs should invest in awareness creation of staff on information security and secure top management commitment on ISMS. Finally the MDAs should prioritize ISMS within their respective strategic planning structures.

CHAPTER ONE

INTRODUCTION

1.1 BACKGROUND

In line with global aspiration for sustainable development, the African Union has through its strategic framework for transformation of Africa's socio-economic status identified a number of development priorities over the next fifty years as espoused in the African Union Agenda 2063. This policy mechanism builds on previous and existing continental initiatives for growth and social progress.[1] Effective implementation of the Agenda and other related development targets requires coherence and complementarity of local, national, regional, continental and global efforts. It also requires policy makers to be conscious of and realign accordingly with changes in the operating environment.

The dawn of globalization and information society has brought forth unprecedented conditions for bridging growth disparities.[2] This includes technological innovations and increased need for re-engineering of government operations through the establishment of transparent, efficient and effective systems of governance. According to Ghavifekr and Rosdy (2015), in the 21st century, technology serves as the highway for knowledge exchange in many countries. [3] The transformation within the security sector has, among others, seen the emergence of Information

[1] African Union Commission. *Agenda 2063: The Africa We Want*, (Addis Ababa: African Union Commission, 2015), 2

[2] Gianluca C. Misuraca. *E-Governance in Africa, from Theory to Action: A Handbook for Local Governance*. (Ottawa: International Development Research Centre, 2007), iii

[3] Simin Ghavifekr and W.A.W. Rosdy. *Teaching and Learning with Technology: Effectiveness of ICT Integration in Schools*. International Journal of Research in Education and Science (IJRES), 1(2), 2015, 175

Security Management System (ISMS) as a vital management tool. ISMS is a process based approach to management that focuses on protecting the confidentiality and integrity of information as well as accessibility to data and information systems.[4] The ISMS approach not only emphasizes the significance of recognizing an entity's data protection needs but also underlines the need to create policies and data protection objectives, implement as well as administer guidelines to govern security risk of corporate information, oversee and analyze information system's performance and efficacy and also continuous improvements based on measurement of objectives. It is an orderly and structured approach to information management. The approach thus constitutes a segment of general governance system, with emphasis on business risks assessment, so as to determine, implement, oversee, evaluate, sustain and enhance data protection.[5]

Information security in relation to ISMS is a couple of measures instituted to aid in the management of policies, processes and also tools which are used in detecting, documenting, preventing and mitigating threats to digital and non-digital information. Information assets relate to not only information itself but also information sources that facilitate management of information.[6] Event refers to any discernable security-related occurrence that may occur in a system or in a network. It may include users who attempt to connect to an information exchange system, network protocols receiving web page requests, individuals accessing various communication platforms such as emails or even firewalls that are trying to block connection attempts. Adverse events are those events which usually have negative consequences, for

[4] E.Blackwell. *Building a Solid Foundation for Intranet Security*. Information Systems Management, Spring 15, 2 (1998), 26

[5] International Organization for Standardization. *ISO/IEC 2700 Standards on Information Technology, Security Techniques, Information Management System Requirements*, 2005, 2.

[6] Per Oscarson. *Information Security Fundamentals*. (Orebro University, 2014), 2.

instance, unauthorized accessibility to sensitive data, unauthorized use of system privileges, package floods, system errors and execution of malware that usually destroy data.[7] Information security incident refers to any suspected attempt, any successful or imminent threat with illegal access and use, alterations as well as disclosure, breach or even data modification. It also refers to the interference with any operations of the information technology and violation of policies related to security of information. Such incidents include computer system intrusion, any use of other users accounts or system privileges without the authorization from the users, improper disclosure of sensitive institutional data, and effecting of unauthorized changes to computer software.[8] A serious incident is an occurrence that could bring about substantial harm to organizational resources, services and/or stakeholders. An incident is designated as serious if it, among others, involves potential, accidental or other unauthorized accessibility or disclosure of sensitive information, involves issues of criminal nature or may culminate into litigation or regulatory investigation, may disrupt critical services, is likely to trigger public interest or is likely to harm the reputation of the organization.[9] A security breach, also known as security violation refers to incidents that may result to unauthorized access to applications, networks, data, services or even bypassing of the set security mechanisms.[10] It normally occurs when one enters a private perimeter illegitimately. Fred Cate (2008) defines security violations as constituting equipment theft such as personal computers or hard drives as well as peripheral storage devices such as pen drives that has information, irrespective of whether or not the information was accessed.[11] Sensitive information implies information whose unauthorized

[7] Paul Cichonski et al. *Computer Security Incident Handling Guide*. (Gaithersburg: National Institute of Standards and Technology, 2012), 6.
[8] University of Michigan. *Standard Practice Guide Policies: Information Security Incident Reporting*, 2016. 1
[9] Ibid., 2
[10] Dale Janssen. *Security Breach*. https://www.techopedia.com/definition/29060/security-breach (Accessed on March 15, 2018)
[11] Fred H. Cate. *Information Security Breaches: Looking Back and Thinking Ahead.* (The Centre for Information Policy Leadership, Indiana University, 2008), 1

access may result into very negative results with adverse effects on the organization reputation, resources are even to the individuals themselves.[12] Incident management refers to the techniques of analyzing the condition of an activity in an organizational entity so as to help in the determination of the extent of the problem and its impact to the organization or business entity. Incidents could be viewed as events that call for management intervention. To ensure the entity is capable of tackling the vulnerabilities, it is important for it to have reliable sources of information. This information is normally incorporated as part of corporate response which is a process through which analysts identify and eradicate an incident and finally recover vital information from the incident. It is the onus of the department mandated to manage incidents to make certain full conformity with the service level agreements whenever they are quantifying and relaying response time. Management of incidents includes data forensic, that is, the potential to formulate, reaffirm as well as safeguard information purposely to conform to the law.[13] An organization's security management is guided by procedures and policies. These form the roadmap of what is permissible and what is prohibited. Responsibilities associated with information security include the establishment of business processes that are used in protecting information assets of an organization.[14] Information security programs are constructed so as to assure confidentiality and integrity of data and presence of information technology in the organization. These objectives are set to guarantee that sensitive information concerning the entity is not conveyed to individuals not authorized to access the information, no unauthorized modification is made on the data and that the data is accessed with ease by authorized parties.

[12] University of Michigan. *Standard Practice Guide Policies: Information Security Incident Reporting*, 2016. 2
[13] Margaret Rouse. *Information Security*. http://searchsecurity.techtarget.com/definition/information-security-infosec (Accessed on March 15, 2018).
[14] Ibid.

A number of theoretical perspectives have been propounded in a bid to grasp the dynamics of information security on organizational performance. The most pronounced information security theories include social technical system theory, social cognitive theory, distributed cognition theory, activity theory and general deterrence theory.[15] The social technical system theory looks at organizational systems as comprising of the social and the technical components, which are independent but very interactive in nature.[16] The social component of this theory takes into account people and their attributes besides their interactions in the organization structure while the technical component takes care of the procedures and tasks being performed in the organization and the technology being employed in the transformation of various inputs into finished products. The activity theory postulates that human activities are usually aimed at the accomplishment of particular results with the aid of both resource and artifacts.[17] Activities form the foundation of analysis and these include mediatory artifacts. The principal goal of human pursuits is production of particular artifacts for the purpose of translation into outcomes and this is the reason as to why a community of subjects involves division of labor towards attainment of certain objectives. These activities are mediated by certain tools, rules and conventions of the society and the surrounding which puts the boundaries through which the activities should be performed. The distributed cognition theory intimates that cognitive functions ought to be perceived in occurrences that are distributed in nature where all cognitive attributes are addressed extensively from various point of views that is the social, organizational and cognitive perspectives.[18] This cognitive phenomenon is distributed in structures where people and their

[15] M.L. Markus and C. Saunders, "Looking for a Few Good Concepts and Theories for the Information Systems Field," MIS Quarterly, 31 (1), 2007, iii-vi.

[16] S.H. Appelbaum. *Social-Technical Systems Theory: An Intervention Strategy for Organizational Development*. Management Decision Journal, 35(6), 1997, 452-463.

[17] M. Gupta. *Activity Theory Guided Role Engineering*. Proceedings of 14th Americas Conference of Information Systems, Toronto, Canada, August 14-17, 2008.

[18] N. Kittur, N. *Cognition, Computation, Design*. 2006. http://www.kittur.org (Accessed April 23, 2018).

interactions, artifacts, internal and external representations are considered collectively as opposed to separately. This theory presumes that cognitive properties consisting of various individuals will differ from individual personal cognitive properties.[19] Distributed cognitive approach is used in information security, where the information security issues should be associated with the cognitive attributes of individuals. The focus of general deterrence theory is sanctions and disincentives against criminal acts and it is adopted from the field of criminology.[20] Information systems safety approaches and techniques have the ability to prevent any cyber criminals and individuals with ill intent from committing unlawful cyber acts. Punishment should be inhibited to anyone aiming at committing any act that breaches the security of information. This theory is very useful in the establishment of security policies and the assessment of the system's risks. The social cognitive theory deals with people's judgments and in its application in information security system research, computer self-efficacy is used in relation to security self-efficacy.[21] For instance, the relationship between system librarians' educational preparations and the efficacy of implementation of information security mechanism is thoroughly examined and the necessary training is offered where necessary. It thus involves examination of information security systems and measuring their effectiveness. The specific theory applied in this study, nevertheless, is the systems theory of management. This is in regard of the broader perspective of how interactions between the various sub-systems within an organization, including the information sub-system, enable the organizational system to effectively deliver its mandate. A detailed analysis of this theory is reflected under the theoretical framework section of this paper.

[19] Yvonne Rogers, *A Brief Introduction to Distributed Cognition*, Interact Lab, School of Cognitive and Computer Sciences, University of Sussex, August, 1997

[20] A.B.J. Cohen and D. Nagin (Eds.). *Deterrence and Incapacitation: Estimating the Effects of Criminal Sanctions on Crime Rates*. (Washington, DC: National Academy of Sciences, 1978). 431

[21] Kittur, op.cit.

This study is, therefore, premised on an understanding that attainment of desired development objectives requires a holistic approach bringing on board all factors that play a role in socio-economic transformation of Africa.

1.2 PROBLEM STATEMENT

Over the recent past, the world has witnessed a significant number of cases concerning breach of information security. According to Qingxiong Ma et al (2009), at the turn of the century, information infrastructure faced increased security threats as compared to any period in history.[22] An article contained in *The Economist* magazine of 7th November, 2015 further indicated that in the period of 2005 to 2015, more than 4,500 information security violations involving approximately 675 million records had occurred.[23] This violation of information assets has also been reported in Africa often impacting negatively on the survival and socio-economic development of individual states. Deriving from the Africa Cyber Security Report of 2017, Francis Waithaka (2018) points out that the annual cost of cyber attacks in Africa and Kenya is USD 1.048 trillion and USD 210 million, respectively.[24] These cases of data breaches have occurred across different economic sectors including security, finance, retail, medical services, communication and online service providers.

Under the circumstances, Government Ministries, Departments and Agencies (MDAs) are exposed to varied security threats in the course of discharging their respective mandates. This

[22] Qingxiong Ma et al., "An Integrated Framework for Information Security Management," *Review of Business* Journal, Volume 30, Issue No. 1 (2009)
[23] Lois Evans, "Protecting Information Assets Using ISO/IEC Security Standards," *Information Management Journal*, November-December 2016.
[24] Francis Waithaka. *Insights from Africa Cyber Security Report*. https://digital4africa.com/2018/04/20/insights-africas-cyber-security-report/ (Accessed June 23, 2018)

includes exposure to cases of fraud, espionage, fire, flood and sabotage from different sources. These threats have particularly served to give insights on the vulnerability of the MDAs and hence the need to institute appropriate measures to safeguard information and information systems. Implementation of ISMS is in this regard considered as one avenue through which the MDAs could be able to address the security breach concerns.

This study sought to determine what are the basic and key success factors of an ISMS? It also sought to establish what common attributes exist between the Kenyan public sector policy framework and the ISMS industry best practices? Lastly, the study focused towards establishing is there a linkage between ISMS and national development?

1.3 OBJECTIVE

The principal aim of this research was to analyze the contribution made by ISMS in the realization of national development agenda.

The specific objectives were:

(a) To examine key issues and factors influencing an effective ISMS.
(b) To evaluate Kenya's institutional and policy framework on information security and ISMS.
(c) To assess the extent and effect of application of ISMS standards in the Kenyan public sector policy environment.

1.4 JUSTIFICATION OF THE STUDY

Research focusing on implementation of ISMS amongst Kenyan public sector entities has not been comprehensively undertaken, despite the ever-rising growth and reliance on ICT systems. This study explores the public sector information security control environment in Kenya. By identifying and analyzing the existing gaps within the policy environment when measured against best practices and more specifically by proposing a benchmark for efficacy in information security management, the study makes meaningful contribution to national level and consequently advancement of the African region. The research also enhances knowledge in the sphere of information security and brings out areas of knowledge gap for purposes of future studies.

The study will specifically add value in the following areas:

(a) It will generate a better insight to pertinent issues regarding ISMS.

(b) It will enable managers of MDAs and other relevant stakeholders to appreciate the relationship between ISMS and national development and the potential harm that information security transgressions can cause to a country.

(c) It will enable public sector policy makers to rethink and review existing security strategies with the purpose of setting up a reliable IT based security infrastructure for sustainable development.

(d) It will offer more insights that will supplement on the initial understanding in the realms of data protection and stimulate further research in this salient area of study.

1.5 LITERATURE REVIEW

This section provides key highlights on themes relating to the three specific study objectives. This includes an analysis of previous studies conducted within the confines of the research area. It draws from a review of secondary data on the subject matter.

1.5.1 HISTORICAL DEVELOPMENTS

The need to protect computer systems was first identified during Second World War when mainframes were first introduced and employed to assist in computations for communication code breaking.[25] In the older times of the computer, the instances of computer security violations were minimal as a result of numerous factors. Firstly, computers at the time were very costly, hence they were not popular and those that existed were heavily guarded. Secondly, the era was also characterized by a limited number of individuals with advanced programming skills since it was a relatively new concept and the machines were encoded in complicated codes. Additionally, the principal emphasis on computer protection at the time was the dependability of the limited and costly computer systems. In fact, information safety was realized primarily via controlling physical computer access.[26] Numerous layers of security were implemented to protect these mainframes and preserve the integrity of data stored therein. Accessibility to sensitive military zones was, for instance, controlled by key passes, identification badges, facial recognition and authentication of authorized staff was carried out by security guards. The mounting need to uphold national security consequently inspired more complex and

[25] Cengage Learning. *Introduction to Information Security*. https://www.cengage.com/resource_uploads/downloads/1111138214_259146.pdf (Accessed on March 20, 2018).

[26] Y. Cherdantseva and J. Hilton, "*The Evolution of Information Security Goals from the 1960s to Today*", Academic Paper Presented at Cardiff University, February, 2012, 10.

technologically sophisticated IT security safeguards. Initially, information security was largely a direct process consisting primarily of basic document categorization schemes and physical security. The main security threats were primarily theft of equipment, sabotage and espionage against system products.[27]

The 1970's were characterized by the advent of personal computers.[28] However, very little consideration was made with regard to information security at the time. Computer devices were isolated and managed by one person and they also had district software. Evidently, the potential risks to information increased tremendously in the later phase of the 70's as a result of the advent of affordable and universal software for computers.[29] Subsequently, as the software and hardware components became cheap and effective, the question of information security shifted from the information processing of computers to the data.. This implied that the purpose of data security discipline was altered in order to address the new concerns. Whilst, initially computer dependability was mostly emphasized, in this phase, privacy, integrity and availability were prioritized. This change in priorities from safeguarding computers to protection of data and the consequent change of security discipline goal ushered in the information security concept.[30] The advent of microprocessor brought about personal computers concept and a new age of computing. The new age of computing was effected by the invention of microprocessors which were installed in personal computers making the personal computer the workhorse of modern computing and moved it from data center. The decentralization of data processors in the 1980s is what instigated the rise of networking, interconnection of personal computers and the mainframe,

[27] Cengage Learning. *Introduction to Information Security*. https://www.cengage.com/resource_uploads/downloads/1111138214_259146.pdf (Accessed on March 20, 2018).
[28] Y. Cherdantseva and J. Hilton, "*The Evolution of Information Security Goals from the 1960s to Today*", Academic Paper Presented at Cadiff University, February, 2012, 11
[29] Ibid.
[30] Ibid., 12

which helped the whole computing community combine their resources so that they could work effectively.[31]

It is at the later phase of the 20th century when the network of computers became more popular, just as the urge or need to connect computer network to each other.[32] These efforts occasioned arrival of the internet, the first global network that was ultimately made available for use by the public. In the 90's, there occurred an explosion that propelled the internet and world wide web phenomenon across the globe.[33] Before then, it was only used by the government, industry professionals and the academia. This explosion enabled connection of computers with capacity to reach phone lines or internet Local Area Network (LAN). Internet commercialization also enabled global accessibility and internet uses have increased as well. As computer networks expanded, the capability of physically securing networked computers became invalidated which implied that the risk to data stored was increasingly vulnerable to information security risks.[34]

In recent times, numerous unsecured computer networks are able to continuously interact with each other with the aid of the internet. The safety of information stored in a computer is thus dependent on the security status of other computers within the network. There have been increased awareness concerning the importance of improving information security and people have also appreciated the fact that information security is vital for national security. Nowadays, governments and companies have invested greatly in protecting computer enabled control systems of utilities and other critical infrastructure due to the escalating levels of cyber-attacks.

[31] Cengage Learning. *Introduction to Information Security*. https://www.cengage.com/resource_uploads/downloads/1111138214_259146.pdf (Accessed on March 20, 2018).
[32] Richard Oppenheim, *"Technology Trends: Part 1: All the Time, Everywhere," Searcher*, May 2010, http://www.questiaschool.com/read/1G1-225589445/technology-trends-part-1-all-the-time-everywhere.
[33] Ibid.
[34] Cengage Learning, op.cit.

There is also growing concern regarding some nation-states being entangled in information warfare and the possibility of the cyber-attack menace extending to business and personal information systems if left undefended.[35] According to Burcu Bulgurcu et al (2010), the overreliance on information Technology systems by companies necessitates effective governance of threats related to the systems. They further observe that today, information related risks pose a huge problem for numerous entities because these threats potentially bear adverse eventualities, ranging from compromising of credibility, huge financial losses as well as corporate liability.[36] Guaranteeing data security has therefore topped in the list of management priorities in many organizations. Success in securing information can be realized in the instance where organizations invest not only in socio-organizational resources but technical resources as well.

As information security focus moves to personal and institutional point of views, employee adherence to set safety regulations has become a fundamental socio-organizational resource because employees are considered as being vulnerable in relation to information security. Corporate entities formulate data security regulations to guide on safeguarding of information assets whereas staff members employ information systems in discharging their jobs. Nonetheless, whilst formulating policies and guidelines provides an important foundation, it is correspondingly important to ensure employees' compliance with them.[37] Therefore, understanding factors that inspire employees to adhere to their organizations' security policies is

[35] Cengage Learning. *Introduction to Information Security*. https://www.cengage.com/resource_uploads/downloads/1111138214_259146.pdf (Accessed on March 20, 2018).
[36] Burcu Bulgurcu, Hasan Cavusoglu and Izak Benbasat. *Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness*. MIS Quarterly, Vol. 34, No. 3 (Management Information Systems Research Center, University of Minnesota, September 2010), 524.
[37] Ibid.

essential in helping help information security managers diagnose deficiencies and provide them with strategies to resolve behavioral challenges in the management of information security.[38]

1.5.2 NATURE OF THREATS

Global dependence on information technology continues to rise each passing day. Companies in recent times cannot function devoid of computers as well as computer related protocols. This dependence has brought about increasing possibility of manipulation of technology to the disadvantage of an organization's ability to function.[39] The global security threat outlook changes remarkably with time.[40] Threats to information come in different forms.[41] Possible threats that an organization may encounter include those of hackers and crackers, authorized insiders, hactivists, script kiddies, information warfare and cyberterrorism. Hackers and crackers are individuals that engage in acts that are aimed at exploring and possibly undermining the IT infrastructure of their targets. Hacking has to do with altering of the computer software and hardware so as to achieve an objective outside originally intended purpose. On its part, cracking involves illegally trying to access a software purposely for distribution. It entails interference with the software protection methods for instance piracy safeguards, hardware keys, serial numbers, date checks, among other security features.[42] Authorized Insiders are legally authorized individuals given access privileges to the IT infrastructure but deliberately perform improper operations. Hacktivism is the tendency

[38] Burcu Bulgurcu, Hasan Cavusoglu and Izak Benbasat. *Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness*. MIS Quarterly, Vol. 34, No. 3 (Management Information Systems Research Center, University of Minnesota, September 2010), 524.

[39] Lawrence D. Dietz. *Information Security Management in the 21st Century*. (California: Symantec Enterprise Security, 2013), 3.

[40] Olavsrud Thor. Information Security Threats that will dominate 2018. Computerworld Philipines, Online Edition 1, Business Source Complete (Accessed June 1, 2018)

[41] Margaret Rouse. *Information Security*. http://searchsecurity.techtarget.com/definition/information-security-infosec (Accessed on March 15, 2018).

[42] Yogita Negi. *Pragmatic Overview of Hacking and Its Counter Measures*. Proceedings of the 5th National Conference, Bharati Institute of Computer Applications and Management, New Delhi, India, March 10 – 11, 2011

of hacking a computer network or a website in order to relay a message of political and/or social nature.[43] Unlike the case of a malicious hacker who unlawfully accesses a computer with the intention of stealing private information or causing other damage, hacktivists get involved in similar kinds of destructive activity to highlight social or political causes.[44] Script Kiddies refers to stereotypical teenagers or youthful hackers, who are motivated by hunting or defeating other technological opponents. They usually have adequate time and access to the computer though they lack other technical skills and they are therefore largely dependent upon the growing hacking equipment inventory, which can be accessed with ease from numerous internet websites.

Information Warfare is the attack against a state's infrastructure by another state, possibly through the military. Information Warfare is subdivided into Computer Network Attacks (CNA), Computer Network Exploration (CNE) as well as Computer Network Defense (CND). CNE includes measures by which adversaries use, inter alia, network merits, characteristics and advantages towards their desired end. For instance, this could encompass the concealing of messages or employing applications for ill intent on an organization or target. The CNE may at times encompass conservative approaches, for instance, the acquisition of information and passwords or nesting of destructive codes within the IT configuration for use at a later stage.[45] Cyber-terrorism bears same features as Information Warfare since it utilizes similar kinds of action. It however deviates from information warfare on the principle that the wrongdoer is not necessarily a country but some form of association for instance an organized terrorist group. Denning (2000) looks at Cyberterrorism as the consolidation of terrorism and cyberspace and

[43] Lawrence D. Dietz. *Information Security Management in the 21st Century*. (California: Symantec Enterprise Security, 2013), 3.
[44] Dale Janssen. *Hactivism*. https://www.techopedia.com/definition/2410/hacktivism (Accessed on April 6, 2018)
[45] Lawrence D. Dietz. *Information Security Management in the 21st Century*. (California: Symantec Enterprise Security, 2013), 4.

describes it as an illegal attack or threat to attack computer networks and stored information when this is done for intimidation purposes or to force governments or citizens to support political or social objectives.[46] For an attack to be considered a cyber-terror, it should be capable of provoking violence against people, property and also have and ability to cause fear. These include events that lead to explosions, plane crashes, among other severe economic losses.[47]

1.5.3 EMERGING ISSUES ON INFORMATION SECURITY

Computer attacks have for quite some time been considered as being unidirectional in nature. The recent past has, nonetheless, been characterized by blurring of the traditional axis of attack. Nowadays, threats to information security come in ways of hackers, crackers, legitimate users performing unauthorized acts, viruses and worms and by exploration of the product vulnerability.[48] Threats from these directions are dangerous and today, it is not unusual to find a combination of one or several threats being performed at the same time.[49] This is what complicates the situation and makes it somehow stressful to overcome the threats. Consequently, many entities have resorted to revision of their approach and taking a turn towards effect based strategies purposely for the reduction of the negative effects.

The nature and structure of IT amongst organizations is currently more vulnerable to cyber threats for diverse reasons. The business landscape is now increasingly sophisticated owing to the addition of software and other related components into the mix. There also exists multiple

[46] D. Denning,, *"Cyberterrorism",* Testimony Before the Special Oversight Panel of Terrorism Committee on Armed Services, US House of Representatives, 23 May 2000.
[47] Margaret Rouse. *Information Security*. http://searchsecurity.techtarget.com/definition/information-security-infosec (Accessed on March 15, 2018), 4
[48] Ibid., 5.
[49] Ibid.

applications and the drive for the optimization of legacy systems with the use of modern technology in IT is yet to be realized. Further, there are new devices and also wireless LAN networks and all these items whenever added to the IT mix, they make it even harder in management of information security.[50] Further still, there currently exists a paradigm swing in IT infrastructure. Businesses and organizations are now changing from the closed information technology infrastructure to embracing open access for their employees, customers, contractors and other institutional stakeholders.

Given the fact that security products have been largely designed in a manner that they thwart a particular threat and not a combination of one or two forms of threats, these changes have made it extremely difficult for businesses to secure their entities fully especially when it comes to information assets. Institutional security designs normally consist of products from various retailers that create log and alarm information in numerous languages and formats. This makes it hard for an enterprise to get the overall outlook of the security given the heterogeneous data generated by those devices that have been acquired from different vendors. The need to have security control across the business entity has been due to the blurring of the traditional corporate perimeter of the organization.[51]

For a long time, information security was viewed by management as largely a technology issue.[52] The solution was seen as one of selecting appropriate software and hardware apparatus and designing an architecture that would aid in the securing of the organization's information assets.

[50] Margaret Rouse. *Information Security, 5.* http://searchsecurity.techtarget.com/definition/information-security-infosec (Accessed on March 15, 2018), 5
[51] Ibid
[52] Dutta, Amitava and Roy, Rahul, "*The Dynamics of Organizational Information Security*" (2003). ICIS 2003 Proceedings. 87. On http://aisel.aisnet.org/icis2003/87 (Accessed on 18th March, 2018)

Hence, it was viewed as a responsibility of the IT department and security related expenditures were seen as a necessary evil. This emphasis on technology solutions still remains. However, over time, it was evident that technology solutions must be supported by appropriate organization structure, management policies and strategy in order to realize effectiveness. For example, the best firewall provides little protection unless the employee termination procedure includes immediate cessation of all access privileges to information. It is common to see cases where employees' access rights have remained active long after they have left an organization or where employees have revealed confidential information over the phone, avoiding secure firewalls. Proper background checks, continuous awareness and security training programs and senior management support are thus all needed in addition to technology.[53] In other words, the predominant perspective of organizations' information security is moving to a position that recognizes it to be an outcome of interaction between technology and organizational factors.

The emerging technological trends have altered the manner in which business is conducted.[54] With the rapid spread of internet commerce, accompanied by an increasing incidence of cybercrime, information security concerns have now reached the boards of many, if not most, organizations. Losses resulting from operational disruptions, customer confidence and the resultant responsibility from information security incidents are prompting organizations to contemplate ways of crafting appropriate security posture. As computer systems get more sophisticated, prevalent and interconnected, the broader society becomes susceptible to poor

[53] Dutta, Amitava and Roy, Rahul, "*The Dynamics of Organizational Information Security*" (2003). ICIS 2003 Proceedings. 87. http://aisel.aisnet.org/icis2003/87 (Accessed on 18th March, 2018)

[54] Charles Jonscher, "Chapter 1 an Economic Study of the Information Technology Revolution," in *Information Technology and the Corporation of the 1990s: Research Studies*, ed. Thomas J. Allen and Michael S. Scott Morton (New York: Oxford University Press, 1994), 5

system structures, attacks on computer systems and accidents that disable the systems.[55] Towards this end, it becomes necessary to understand the mechanisms through which information security is either compromised or reinforced in organizations. Management can then take deliberate measures aimed at weakening the former and strengthening the latter to achieve a suitable balance. This paper pursues this line of thought by conceptualizing an information security model that portrays underlying mechanics.

1.5.4 INFORMATION TECHNOLOGY AND NATIONAL DEVELOPMENT

Science and Technology affects all aspects of contemporary society. As pointed out by Lee-Roy Chetty (2012), there is hardly an industry that has not been impacted by the growing hi-tech revolution.[56] The application of technology distinguishes nations that have the capacity to appropriately address the issue of poverty through expanding and advancing economic conditions and the nations that are unable to. However, the level to which growing nations arise and impose themselves is dependent on the capability to comprehend and objectively incorporate scientific insights as well as creative application of technology. Innovation is a key driver of growth technology in addition to promoting better standard of living in a country. The inputs constitute below half the differences in per-capita revenue across countries.[57] The remainder is attributable to the failure in the application of new concepts to increase productivity, for instance, by opening infrastructure backlogs. Integrated supply modules can revolutionize economic improvement through facilitating accessible and less costly utilities in all areas of humanity.

[55] National Research Council. *Safe Computing In the Information Age.* (Washington: National Academy Press, 1991), 1.
[56] Lee-Roy Chetty. *The Role of Science and Technology in the Developing World in the 21st "Century*," Institute for Ethics and Emerging Technologies Journal, October 3, 2012.
[57] Ibid.

Advances in information technology and science have greatly changed the manner in which individuals interact and negotiate business with significant influences on advancement of the economy. [58] Information and its related technologies have become quite important to business success such that information is often regarded as an independent aspect of production and at par with capital, land and labour.[59] Science and technology are key factors for development because these two factors, with their revolution over time, support economic progress in improving education, health and infrastructure systems.[60] The rapid dispatch of information internally, at the regional and global level has facilitated the expansion of commercial activity to greater heights, making it possible for individuals to transact anywhere and small businesses being able to sell products much easily, since they can easily communicate and fix agreement. Technology is a resource and tool of knowledge and also the new platform for doing business.[61] The evolution of e-commerce has facilitated and fostered convenience for individual buyers to choose products electronically as well as effect immediate payments.

Science and technology has also enabled scaling up of agricultural activities geared towards promoting food security and by extension human security. Use of technological tools in agriculture has specifically contributed towards improvement in agricultural productivity and better access to input and product markets.[62] Mechanized farming continues to play a critical part in sustaining food security. Through science and technology irrigation farming has been realized to avert the unpredictable weather conditions with the objective of improving crop

[58] Lee-Roy Chetty. *The Role of Science and Technology in the Developing World in the 21st "Century*," Institute for Ethics and Emerging Technologies Journal, October 3, 2012.
[59] Stephen D. Tansey, *Business, Information Technology and Society* (London: Routledge, 2003), xv
[60] Chetty. op.cit.
[61] George Kozmetsky, Frederick Williams, and Victoria Williams, *New Wealth: Commercialization of Science and Technology for Business and Economic Development* (Westport, CT: Praeger, 2004), 18
[62] Blessing M. Maumbe. International Journal of ICT Research and Development in Africa, Available at: www. Igi-global.com, 2010.

yield. Use of satellite has enabled the agricultural sector to undertake agricultural processing whereby the type of soil, crop yield and use of fertilizer may be determined through the satellite link. Technology has further enabled production of different types of fertilizers thereby facilitating greater crop yield. Additional benefits arise when farmers use ICT by way of improved accessibility to information on the agriculture and food industry, coupled with networks of knowledge and an increment in job opportunities. This is made possible, inter alia, through enhanced communication channels among different stakeholders including farmers, suppliers, and marketing firms.

Further still, Science and Technology has contributed massively to the health sector. Some natural herbs have been converted to drugs with the aid of modern equipment and used in hospitals and pharmacies. In May 1990, a resolution was passed in the 43rd World Health Assembly where the Director-General was tasked to, on regular basis, organize for monitoring and evaluation of technological and scientific developments that could possibly improve health care or its delivery, particularly amongst developing nations. The principal aim was to guarantee that potentially vital developments are acknowledged and also ensure that inventions and innovations for health care purposes were encouraged.[63] With the assistance of technology, biomedical research has progressively generated complex and voluminous amounts of relevant information on health.[64]

New technological trends have also occasioned fresh multilateral collaborative ventures in various aspects of state-society relations, growth sustainability, governance, peace and conflict

[63] World Health Organization, "Emerging Science and Technology for Health," *Bulletin of the World Health Organization*, Volume 71, Issue No. 6 (1993)
[64] "Biomedical Information Science and Technology Initiatives," *Environmental Health Perspectives Joutrnal.* Vol 108, Issue No. 11 (2000)

and global security. In regard to peace and conflict, new technologies can aid in avoidance of conflicts by bridging the gap existing between warning and response, facilitating peacekeeping with new instruments relevant to increasingly sophisticated environments and reinforcing peace building efforts through empowerment of local actors. New technologies and internet governance constitute an area where future contribution of multilateral actors comes into greater focus.[65] Whether in peace and conflict, sustainable development, relations between state and society, international security or cyber-space, new technologies have changed the way the UN and multilateral institutions operate in the contemporary globalized world.

The later phase of the 20th century was characterized by significant strides in military technology. The superpower rivalry that arose after 1945 served to propel technological competition resulting in outstanding outcomes within a limited time frame. The spread of new technology gave rise to new and serious concern regarding propagation of Weapons of Mass Destruction technologies to individuals bearing ill intentions. Certainly, tremendous advancement in ICT over the course of history has given rise to numerous possibilities such as the application of technology in strategic operations.[66] Today's emerging technologies, for instance nanotechnology, advanced computing and biotechnology are tipped to revolutionize the world and thus the shape of international relations and military affairs.[67] Improving speeds of computers, shrinking hardware and advent of creative software strategies provide additional options and opportunities. Information Technology has in fact transformed the warfare

[65] M. Tyler, J. Hughes and H. Renfrew. *Kenya: Facing the Challenges of an Open Economy*. In E.M. Noam (Ed.), Telecommunications in Africa, (UK: Oxford University Press, 1999), 79-112.
[66] Amitav Malik. *Technology and Security in the 21st Century: A Demand-Side Perspective* (Oxford: Oxford University Press, 2004), 17
[67] Wilson S. Wong, *Emerging Military Technologies: A Guide to the Issues* (Santa Barbara, CA: Praeger, 2013), 1

landscape for instance through emerging trends in not only network-centric commands but also management philosophies.[68]

The other anticipated major technological trend is the increased application of outer space in security and defense strategies. Space technology is currently employed by the defense forces, specifically for technological support in surveillance and communication. These undertakings have had immense effect on how security and defense strategies are perceived. The expected launch of arms that are energy directed as well as the potential increment in military utilization of satellite technology for warfare will transform combat and show of might among formidable nations.

The emerging technological trends and advancements in defense strategies also depict significant strides towards the realization of miniaturization, increased efficacy and reliability. With the improvement of efficiency and the reduction in size of arms, distribution mechanisms and operation dynamics are now very flexible thereby providing even more options to the user. In recent times, the defense forces are embracing significant advancements in electronic and surveillance technology in war as well as development of arms and command, management and communication.[69] The diminishing weight and size of strategic warheads are examples of ways in which technology has simplified an intruder's work whilst at the same time complicating the task of the defense forces, generating increased demand for the embracing of emerging technology in a bid to address the high risk level.[70] The improvement of weapon delivery accuracy technology and the increment in the fatality estimates of emerging weapons has

[68] Amitav Malik. *Technology and Security in the 21st Century: A Demand-Side Perspective* (Oxford: Oxford University Press, 2004), 17.
[69] Ralph Sanders, *International Dynamics of Technology* (Westport, CT: Greenwood Press, 1983), 4
[70] Malik. op.cit.

generated interest in championing for arms that are not nuclear-oriented. In the event that compressed, universal and efficient arms could be deployed over a great reach so as to attain reliable attacks with top notch accuracy on enemy sites, this potential would revolutionize the principal concept of strategic defense. Whilst the advancement in technology could in actual fact aid in the quest to decrease overreliance on nuclear weapons, new technology may give rise to numerous challenges associated with overseeing the conventional organizational capabilities from the perspective of ancient weapons. In order to guarantee improved transparency and reliability of weapon transfer information, emphasis on future weapons or technology regulations will therefore have to change towards cooperative technology-control structure that encompasses every accountable technology owner globally.[71] Technological advancements may compel the current society to reconsider the definition of proliferation and to nations, 'of concern' the need to foster an in-depth comprehension of the feasibility as well as the merits of global nuclear disarmament, attained in an organized and guided manner.

The emerging technology has served to complicate cyber security whilst also transforming the war strategies. New technology has has fostered new modes of exerting lethal strategies for instance through the armed Unmanned Aerial Vehicles (UAVs), including drones, that present new setback and concerns. DeGarmo (2004) particularly observes the fact that UAVs present a potentially disruptive effect on the totality of the aviation system.[72] Whereas there has been a general agreement that the deployment of armed drones is not necessarily outlawed, there is no universal stance on how international regulations can be applied on the forceful use of drones, and issues have been brought up regarding the possible expansion of geographical as well as the

[71] Amitav Malik. *Technology and Security in the 21st Century: A Demand-Side Perspective* (Oxford: Oxford University Press, 2004), 17.

[72] Mathew T. DeGarmo. Issues Concerning Integration of Unmanned Aerial Vehicles in Civil Airspace (McLean, Virginia: The MITRE Corporation, 2004), viii

temporal boundaries of use of force. Additionally, the potential application of drones by non-state actors increases further the regulatory complications.[73] Besides, more broadly used technologies such as mobile devices and internet are vastly applied to aid warfare through fostering communication, informing public choices, intelligence collection, emerging warfare technique training as well as cyber-attack involvement. This ultimately impacts on government policy and organization.[74]

Changes in security are normally slow and implementation of any new security technology has to be given a serious consideration as a collective responsibility involving the government and the society which implies that agreement, coordination and sometimes very long bureaucratic procurement process. With rapid innovations in technology, law enforcement agencies tend to face a daunting task as initially in their way of dealing with the criminals who seem to be more flexible and faster in manoeuvring through the communication systems and end up in establishing more disguised groups on the internet.

Religious fundamentalism and terrorism have spread rapidly globally. This has, in turn, rendered the modern society more susceptible to attacks. Religious fundamentalists and terror factions engage in criminal activities with no affiliations to a given country or global customs. Technological advances have added to the efficacy of extremist groups as well as those that sponsor them.[75] Another interesting trend is that some nations out of considering themselves safeguarded by the deterrent capabilities of Weapons of Mass Destruction, may get a sense of

[73] Heyns, Report of the Special Rapporteur on Extrajudicial, Summary, or Arbitrary Executions, UN Doc. A/HRC/26/36, April 1, 2014; Ben Emmerson, Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, UN Doc. A/HRC/25/59, March 10, 2014.

[74] Ralph Sanders, *International Dynamics of Technology* (Westport, CT: Greenwood Press, 1983), 4

[75] Amitav Malik. *Technology and Security in the 21st Century*. (New York: Oxford University Press, 2004), 18

security and comfort to stealthy champion extremism across state boundaries to address regional disagreements. These emerging and looming issues as well as the possible abuse of technology must accordingly be addressed by the global weapon control community prior to generating into new trends in asymmetric warfare which may compromise global security in unprecedented ways.[76]

Considering the manner in which modern technologies make it hard to apply existing global regulatory instruments from various points of view, there is a need for clarity and general agreement on how to implement these frameworks. In regard to the physical sphere, a considerable role of the multilateral system can be foreseen in establishing the ethos and conditions to regulate foul undertakings of states in the cybersphere as well as via emerging conflict modes.[77]

With the growth of internet networks and the computer industry in general, things have significantly changed over the last thirty years and global communications have attained an unprecedented level.[78] With these developments, huge goals have emerged to give knowledge both interactively and effectively. Modern concepts for instance multimedia and the internet have transformed the foundation of surveillance in security. It has also created spaces for communication and coordination of actions between groups of people located in various geographical locations. There are now more advanced and integrated devices that allow people to

[76] Amitav Malik. *Technology and Security in the 21st Century*. (New York: Oxford University Press, 2004), 16

[77] Heyns, Report of the Special Rapporteur on Extrajudicial, Summary, or Arbitrary Executions, UN Doc. A/HRC/26/36, April 1, 2014; Ben Emmerson, Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, UN Doc. A/HRC/25/59, March10, 2014.

[78] Oliver Masuti. *Impact of IT on Society in the New Century*. http://www.zurich.ibm.com/pdf/news/Masutti.pdf. (Accessed on May 25, 2018).

disregard surroundings.[79] Courtesy of science and technology, it is nowadays possible to attend meetings without being physically present. Business acquaintances in a virtual conference setting can interrelate with one another synonymous with real engagement. The requirement to travel physically has thus decreased significantly.

1.5.5 ROLE OF INFORMATION SECURITY MANAGEMENT SYSTEM

An ISMS is simply a coordinated way of handling valuable information about an organization to keep it secure.[80] It covers people, IT systems and related processes. The certification of an ISMS makes certain that an entity has a mechanism for setting up, operating, maintaining, evaluating and improving the security of information, including customer information being held by the organization.[81] The implemented ISMS guarantees the management of general business risks through the administration of customized security controls with regard to the conditions of the organization, thus increasing people's productivity and improving the corporate image. ISMS is an organizational system that draws from systematic protocols to business threats to determine, implement, oversee, maintain, operate, evaluate as well as enhance data safety.

There are numerous problems in the jurisdictions of data security. These encompass a change of web pages content by intruders, damage to information systems by malicious software and leaks of information from the people concerned. The development and operationalization of ISMS by way of adequate risk assessment against these threats is essential to ensure the general security of

[79] Oliver Masuti. *Impact of IT on Society in the New Century*. http://www.zurich.ibm.com/pdf/news/Masutti.pdf. (Accessed on May 25, 2018).
[80] International Organization for Standardization. *Information Security Management Systems*. https://www.iso.org/isoiec-27001-information-security.html (Accessed on March 23, 2018)
[81] Indian Register Quality System. *Information Security Management System*. http://www.irqs.co.in/information-security-management-system.html (Accessed on February 15, 2018)

information in an organization. An ISMS allows an organization to systematically manage its information resources. By creating the ISMS, an entity can determine the security level needed, create plans, distribute resources and manage systems based on risk assessment, along with individual technical countermeasures for each problem. ISMS's key concept is preserving the integrity, confidentiality and availability of information through the application of suitable risk management processes and giving the stakeholders confidence that risks are managed correctly. To realize this end, it is imperative that the ISMS is integrated with organizational processes and the general management structure.[82]

1.5.6 CHARACTERISTICS OF THE PUBLIC SERVICE

The public sector comprises both public and state managed or publicly financed enterprises, agencies and other entities offering public initiatives, products or services.[83] It entails a growing group of institutions, with the central government at the helm and public enterprises and other agencies at the periphery.[84] Core government includes ministries, departments or state branches that are important components of government structure. Besides, they are accountable and answer to the state authority. Agencies are public institutions that are constituents of government and spearhead implementation of government programmes and/or provision of public, goods or services, but which exist as separate institutions, possibly as legal entities, and operate under some level of independence. [85] In most cases, they are headed by management boards comprising of commissioners, directors or any other officials designated by law. Public enterprises are entities that provide public programmes, products or services. However, they operate

[82] International Organization for Standardization. ISO/IEC 27001:2013 Standard
[83] The Institute of Internal Auditors. Supplementary Guidance: *Public Sector Definition*. December, 2011, 3
[84] Ibid.
[85] Ibid., 4.

independently, that is, free of state control and ordinarily they are equipped with their own distinct revenue sources besides direct funding from the public resources. They can also participate in the private markets in order to generate profits. Nonetheless, in a majority of cases, the foremost shareholder is the state and the organizations adhere to the rules and legislation governing the central government.[86]

According to Schacter (2002), the public sector bears the responsibility of planning of public policies. [87] In other words, public servants translate the vision of elected officials into actionable strategies. The sector is also responsible for implementing government programmes and policies to achieve solid economic development, increasing national income, monitoring public spending and management of accountability.[88] In a developmental state, due to the dominant role played by the government in the provision of the Rostowian pre-condition for takeoff and the comparative weakness of the indigenous private sector, the public sector takes on a much greater position in national development.[89]

The central focus of state and public service agencies is the provision of products and services rather than profit maximization. Throughout the world, the public service differs significantly on account of not only the provisions of the constitution but also on the operational procedures. The models of governance by state and the public service agencies usually involve maintenance by the executive body of a regulatory entity or an equivalent mode of authority. This requires to be considered during the interpretation of financial reports. The sector scope and goods and services

[86] The Institute of Internal Auditors. Supplementary Guidance: *Public Sector Definition*. December, 2011, 4.
[87] Mark Schacter, *Public Reforms in Developing Countries: Issues, Lessons and Future Directions*. (Ottawa: Institute of Governance, 2002), 4
[88] Ibid.
[89] Prof. Stephen Adei. *The Role of Public Service in a Developmental State: Lessons from the Newly Industrialized Countries (NICs) for Africa*. African Association For Public Administration and Management, 30th AAPAM Annual Roundtable Conference, Accra, Ghana 6th – 10th October 2008, 4.

that it provides depends on, for instance, political ideology and the magnitude of the economy.[90] A government-controlled entity could be an organization that provides financial gain for the government where the entity produces goods and offers services at market prices (also known as a corporation) or it could be an entity that does not provide revenue generation for the state, irrespective of the cost implications from the sale of products and services it generates, in other words a non-profit entity. Governments exercise autonomy differently over the separate categories of state entities.[91]

There are five fundamental features of public enterprises. Firstly, we have the issue of state ownership. The ownership of the enterprise must be conferred on the State. It could be a property of a local authority or the central government. Any state instrument could also claim ownership of a public enterprise based on the existing institutional arrangements. Secondly, we have state control, whereby the government oversees the operations of a public enterprise in terms of its overall management and functioning. The Government thus has a direct obligation of managing the undertakings of the enterprise through various ways and means. Thirdly, we have public accountability and this refers to the situation whereby public enterprises owe accountability to the public given that their operations are financed through government revenue. This accountability is implemented through a number of oversight instruments including parliament and its committees, audit bodies and other relevant specialized agencies. Fourth is autonomy and under this, public bodies serve with utmost autonomy under given situations. They are free from external interference in the daily running of the organizations. Lastly is the question of coverage where the scope of public enterprises traverses a wide scope of areas and activities.

[90] International Public Sector Accounting Standards Board. *Key Characteristics of the Public Sector*. International Federation of Accountants, December, 2010), 3.

[91] Taskforce on Harmonization of Public Sector Accounting. *Government / Public Sector / Private Sector Delineation Issues*. Fourth meeting of the Advisory Expert Group on National Accounts, Frankfurt, 30 January – 8 February 2006, 4-5.

The rather obvious distinguishing attribute between private and public service is the fact that in private agencies, the core purpose is the ensuring of maximum profitability as well as value addition in the economy, whereas public sector enterprises might be in pursuit of both profit-making as well as non-profitable objectives.[92] The public service is thus not purely a profitable venture in regard to the commercial implication of the word. Nevertheless, since public sector organizations are not for profit firms, that ought to not direct us into believing that public services managers as well as the employees are not bothered about financial issues. [93] Evidently, as compared to private entities, public service institutions and units wrestle for influence and income.

The other distinguishing attribute of the private and public agencies is the unit of analysis. Other than the public ownership aspect of public service bodies, a vast majority are a segment of a bigger command hierarchy that is sophisticated and hard to distinguish between the various constituents of the system and scenarios where legislations offer minimal help in regard to the situation. For example, public entities, such as directorates of health or research councils collaborate with relevant ministries and also subordinate entities as well as "users". Innovative undertakings in these entities are thus greatly influenced by hierarchy of command decisions made both at the top and bottom levels of the organization. Another vital distinction is the fact that political influence is very profound in public service as compared to their influence in private entities. [94] Legislative decisions influence organizations indirectly, via financial support, regulations and legislation. The public service is by and large influenced by the political class in

[92] Stefan Bogdan Salej. *Models of the State Ownership Function Organization.* Proceedings of the High Level Meeting of State Ownership Authorities, 5th – 6th September, 2011, Ljubljana, Slovenia
[93] Per Koch. *The Difference Between Public and Private Sectors*. The Publin Post Newsletter, No. 7, 2005, 1-2
[94] Ibid.

the shaping of its strategic direction. The strong correlation between the existing governance dimension and financial support of operations signifies a firm relationship between management and ownership on the one side and the development approaches of subsidiary organizations on the other. In terms of management incentives, public managers in general have a higher chance of receiving minimal performance oriented material merits that could potentially influence readiness for risk taking. The general belief is that the public service, under ideal conditions would recruit a limited number of managers that are risk takers as compared to private agencies owing to the presumption in form of entrepreneurial penalties or rewards. [95] Furthermore, it is highly probable that private innovative entities have a higher likelihood to accept "failure" than public institutions.[96] "Failure" in this context refers to innovative programmes and projects that end up not accomplishing the presumed aims. Private institutions may take "failure" as an engraved measure of potentially risky businesses whilst the pressure for economic utilization of public resources, and accountability in the use of public funds, may indicate a vital innovation disincentive. Generally, it would be anticipated that public entities are risk averse relative to the market based institutions, basically as a product of the effective attributes of incentive programs experienced by the two organizational forms. The Australian Auditor General, Ian Mcphee (2005) asserts that this may also be attributed to the relevance of the legal framework that governs public administration and the fact that public funds need to be handled with due care.[97]

[95] Per Koch. *The Difference Between Public and Private Sectors*. The Publin Post Newsletter, No. 7, 2005, 2
[96] Ibid.
[97] Ian McPhee. *"Risk and Risk Management in the Public Sector"*. Public Sector Governance and Risk Forum, September 1, 2005.

1.5.7 STUDIES CONDUCTED ON ISMS

The relevance of information security systems has been documented by various scholars around the world. In a study conducted by Cheol, Jang and Park (2010) on the impact of information security on organization performance in Korea, the findings indicated that incorporation of ISMS helps to prevent intrusions and related damage thereby having a cost saving effect.[98]

In another study, Heekyung Kong et al (2015) explored the impact of adopting the data protection management on institutional performance among the Korean securities firms. The study findings indicated that implementation of ISMS helped to boost the stability of undertakings, consequently translating to an improvement in institutional performance.[99]

In yet another research conducted in 2013 by Amarachi, Okolie and Ajaegbu on the emerging issues and prospects in ISMS under the reflection of the Nigerian socio-economic environment, the findings indicated that information security systems play a crucial role in supporting business operations and thus the need for every organization to have an ISMS that could sufficiently provide support for IT applications and business processes and reasonable assurance.[100]

On the Kenyan front, Sirma, Muiru, and Kipchillat conducted a study in 2014 where they investigated the implications of data protection regulation on security violation instances among Kenyan public institutions of higher learning. The study revealed that a negative correlation

[98] C.S. Park, Jang, S. S., and Park, Y. T. A study of effect of Information Security Management System [ISMS] Certification on Organization Performance. International Journal of Computer Science and Network Security, 2010.10 (3).

[99] H. Kong, H., Jung, S., Lee, I., and Yeon, S. J. *Information Security and Organizational Performance: Empirical Study of Korean Securities Industry*. ETRI Journal, 2015, 428-437.

[100] Amarachi, A. A., Okolie, S. O., and C. Ajaegbu. *Information Security Management System: Emerging Issues and Prospects*. IOSR Journal of Computer Engineering,(2013)

exists between ISMS and security breach cases.[101] This implies that institutions can reduce incidences of security breach by strengthening information security management systems. Another study within the Kenyan context is that conducted by Madiavale Beverly Agosa in 2009 regarding information security management practices and organizational goals amongst Microfinance Institutions (MFIs) in Nairobi. The study sought to establish ISM practices in use by the MFIs, ISM awareness level amongst the various stakeholders in the MFI sector and the extent of alignment of ISM operations with institutional goals. The study findings, among others, indicated that most MFIs had adopted the very basic forms of ISM practices and that the level of awareness of ISM practices within the stakeholder community was generally low. The study therefore underscored the need to enhance knowledge on ISM practices and allocate additional resources towards development and sustainability of ISM practices in the sector. It also recommended for further research linking ISM practices and realization of organizational goals. This partly informs the scope of this study.

1.6 THEORETICAL FRAMEWORK

A theory is an array of intertwined variables, propositions and definitions that provides a logical perspective of occurrences by identifying association among parameters, purposely to explain natural phenomena.[102] Babbie (2004) has also defined a theory as a systematic account of observation that relates to a specific aspect of life.[103] Theoretical frameworks provide rationale for predicting relationships existing among different parameters of a research study. A

[101] Sirma, J., Muiru, M., & Kipchillat, D. C. *Impact of Information Security Policies on Computer Security Breach Incidences in Kenyan Public Universities*. Information and Knowledge Management Journal, Vol. 4, 2014.
[102] Bacharach, S.B., *"Organizational Theories: Some Criteria for Evaluation,"* Academy of Management Review (14:4), 1989, 496-515.
[103] Earl Babbie, *The Practice of Social Research. (*Belmont, CA: Wadsworth/ Thomson Learning, 2004), 43

theoretical framework, therefore, informs various decisions made during the research process.[104] As observed earlier, this study is guided by the Systems Theory of management which looks at relationships between organizations and the respective operating environment.

The Systems Theory, whose principal proponent is Ludwig Von Bertalanffy, is premised on the perspective that relies on linear, cause-and-effect parameters to explain transformation of living organisms. These characteristics are dependent on two foundations. Firstly, that interaction takes place between components, and secondly, that the relationship existing between the different components is linear. In the instant that both conditions are present, the interaction is quantifiable and verifiable through scientific inquiry. The theory advances the notion that organizations, similar to living organisms, comprises of various component subsystems that need to work together in harmony for the success of the bigger system. It, thus, treats an organization as an overarching system consisting of several subsystems.

To understand the Systems Theory, it is necessary to have a fine grasp of the concept system. A system is a collection of different components that interact to form the sophisticated whole. An example to this effect could be drawn from the universe, whereby the universe comprises of components as minute as a sub-atomic matter or as massive as galactic bodies. Individual elements are distinct but synergize to make the universe. According to the Systems Theory of management, organizations are systems encompassing numerous segments for example employees, work groups, commodities, resources, assets, as well as data which, put together, form the complex whole. The success and/or failure of an organization is dependent on interrelations, synergy and interdependence amongst different subsystems. For instance,

[104] D.M. Mertens. *Inclusive Evaluation: Implications of Transformative Theory for Evaluation*. American Journal of Evaluation, 20(1), 1999, 1-14.

individual workers may vary or modify the inputs, included being their own actions, to generate a change within the system.[105] An open system within the organization interacts with the environment in form of inputs, throughputs and outputs. How a field defines the system is the determinant of the kind of interaction.[106]

The systems approach provides a meaningful way of reflecting upon the job of managing. It provides a framework by which internal and exterior factors within the operating environment could be visualized as an integrated whole. It allows for recognizing the rightful place and functions of subsystems.[107] Considering the fact that organizational entities operate within the parameters of complex systems, management via systems concepts fosters a way of thinking which aids in dissolving some of the complexities as well as aiding the managers to appreciate the dynamism of situations and operate with ease in the confines of the perceived surroundings.[108] It is necessary to acknowledge the integrated status of systems, including the reality that an individual system comprises of not only inputs but also outputs and may in this regard be seen as a self-contained bloc. It is equally crucial to note that business structures are constituents of bigger systems that may cut across the entire industry. Further, organizational systems are continuously changing as they are made, operationalized, revised and even eliminated.[109]

[105] Bruce D. Friedman and Karen Neuman Allen. *Systems Theory*. (In Theory and Practice in Clinical Social Work Practice edited by Jerrold R. Brandell, 2010), 3-4
[106] Ibid.
[107] Richard A. Johnson, Fremont E. Kast, and James E. Rosenzweig . *Systems Theory and Management*. Management Science Journal. Vol. 10, No. 2, January, 1964
[108] Ibid.
[109] Ibid.

The theory informs the study since it presents the ISMS as a sub-system that contributes to the organization system through, inter alia, control and protection of information assets. Organizations would in this regard be expected to inspect their respective surroundings and safety standards so as to design appropriate data security regulations, ascertain the degree of data security and evaluate existing risks and controls so as to form an ISMS subsystem that feeds into the global organization system.

1.7 HYPOTHESES

The study sought to test the following research hypotheses:

(a) Enhanced utilization of ISMS will promote development in Kenya.

(b) Information security and ISMS improve the performance of public sector agencies.

1.8 METHODOLOGY

1.8.1 INTRODUCTION

The case study design was applied as the basis for data collection. The study sought a profound understanding of the basic principles of ISMS and its application in Kenya.

1.8.2 STUDY SITE

This study was carried out in Nairobi, Kenya. The primary data was obtained from institutions located within the Central Business District whereas secondary data was, other than internet sources, obtained from assorted information resource centres in the city.

1.8.3 TARGET POPULATION

The population of interest was technical personnel at the Ministry of Information and Communication responsible for public sector ICT policy formulation and implementation.

1.8.4 SAMPLE SELECTION

Key informant interviews were undertaken on five middle level and senior officers (Job Group M and above) at the Ministry. The officers were drawn from the directorate of ICT, where there were a total of fifteen officers falling under the category of Job Group M and above. The directorate was the most suitable department for the research given that it is charged with, among others, coordination of the development, implementation and review of nationwide ICT policies (including security policies), provision of ICT technical support services to MDAs and monitoring performance of the MDAs. The officers shed light on matters concerning national policy guidelines on information security and ISMS and also on performance planning, monitoring and evaluation, thereby enriching the study.

1.8.5 DATA COLLECTION METHODS

This study employed qualitative research methods to gather and analyze data. This method was considered suitable since the study is exploratory in nature and concerned with developing deep understanding of the role of ISMS on development in Kenya. The approach thus enabled generation of detailed data and thereby provided a clear perspective of the research issue.

Research data was collected using both primary as well as secondary data sources. Primary data was assembled via Key Informant Interviews aided by Key Informant Interview Guide. The interview guide was classified into distinct sections to facilitate systematic and timely interpretation of collected data. Primary data collection also involved establishing the level of domestication of ISMS standards within the Kenyan policy environment using the observation check list. The results of key informant interviews were corroborated with interactions with officers from other levels of Government, including the Kenya ICT Authority. Secondary data was on the other hand collected through review of books, journal articles, government reports, previous research papers and articles from relevant websites.

1.8.6 VALIDITY AND CREDIBILITY OF DATA COLLECTION INSTRUMENTS

The instruments of collecting data were shared upfront with the supervisor to ensure their adequacy and reliability. Prior approval was obtained from the supervisor before administering these tools.

1.8.7 DATA PRESENTATION AND ANALYSIS

Data analysis was undertaken through thematic assessment. This involved identification, consolidation and reporting on various ISMS related themes within the qualitative data. This facilitated systematic data organization, description and interpretation and thereafter drawing conclusions.

1.8.8 ETHICAL CONSIDERATIONS

Prior consent was obtained from all individuals participating in this study. Confidentiality on the part of the informants was respected as per their preference. A research permit was also obtained from the National Commission for Science, Technology and Innovation (NACOSTI), a copy of which appears as an appendix of this paper.

1.9 SCOPE AND LIMITATION

This study largely concentrated on Kenya as a case study. It set out to review Kenya's national policy framework on ISMS and further provide a linkage between ISMS and realization of the country's development objectives. In view of resource and time constraints, the research process did not incorporate the entire population of policy makers. Nevertheless, a representative sample of the population was identified for the interviews to ensure reliability of study findings. The primary data was further be corroborated by secondary data sources.

1.10 CHAPTER OUTLINE

This research paper is presented in five chapters. Chapter one encompasses background information and methodology. Chapter two focuses on fundamental issues and factors affecting data security and development in Africa. Chapter three gives insights on the Kenya's institutional and policy framework on information security and ISMS. Chapter four provides an analysis of the extent and effect of application of ISMS standards in the Kenya public sector policy environment. Lastly, Chapter five provides summary, conclusion and recommendations arising from the study.

1.11 CHAPTER SUMMARY

This chapter has provided a general outlook of the area of study, including historical background and emerging concepts in information security. The chapter has also, among others, outlined the research questions/problem statement, study objectives, literature review and the methodology used. In this regard, the study addresses three specific objectives, namely, to examine key issues and factors influencing an effective ISMS, to evaluate Kenya's institutional and policy framework on information security and ISMS and to assess the degree and effect of application of ISMS standards in the Kenyan public sector policy environment. The study objectives were informed by the increasing significance of information security amongst African countries in the face of the realities of globalization. From the review of previous studies and other secondary data sources, it is evident that ISMS holds a central place in the modern-day management practices. There is general consensus that establishment of an ISM mechanism not only helps to safeguard organizational information assets but also contributes towards the actualization of development objectives. The next chapter links this broad outline to specific organizational and developmental issues with specific focus on Africa.

CHAPTER TWO

OVERVIEW OF INFORMATION SECURITY AND DEVELOPMENT IN AFRICA

2.1 INTRODUCTION

This chapter builds on the introductory aspects of data security discussed in chapter one. The chapter highlights key issues relating to information security, including information security trends in Africa. It also provides essential components of an effective ISMS and their applicability to the African context. This includes a review of general information security requirements, key characteristic features and applicable best practices associated with ISMS. The chapter further analyses procedures involved in implementing ISMS, its benefits, challenges, possible mitigation measures and the interface between information security and ISMS and development in Africa.

2.2 APPLICATION OF INFORMATION SYSTEMS IN AFRICA

Following the adoption of the Agenda 2063 framework in early 2015 as the foundation for Africa's long-term socio-economic reinvention, the African Union Summit instructed the African Union Commission (AUC) to formulate the initial Ten Year Implementation Plan of the Agenda.[110] Amongst the flagship programmes and projects envisaged in the Ten-Year Plan is the execution of a Pan-African E-Network. This entails a broad scope of stakeholders and it envisages formulating policies and approaches that result into transformative services and e-

[110] African Union Commission. First Ten-Year Implementation Plan 2014 – 2023 of Agenda 2063. (Addis Ababa: African Union Commission, 2015), 12.

applications in the continent, particularly the intra-Africa broad band terrestrial infrastructure as well as cyber security, making information revolution the foundation for service delivery in the nano and biotechnology sectors and consequently shaping Africa towards being an e-Society.[111] The Plan also envisages increment in accessibility to tertiary and continuing education in Africa by simultaneously reaching out to a big number of professionals and learners in several web sites and creating high quality and relevant Open, Distance and eLearning (ODeL) services to provide the prospective learners with sure access to institutions of higher learning at any given time and place globally.[112]

Besides the above, the African continent has over the recent past pursued the New Partnership for Africa's Development (NEPAD) programme as an avenue towards realization of desired development objectives. NEPAD is a joint United Nations Organization and World Bank project geared towards formulating an integrated socio-economic framework for the revival of Africa. It has three central areas of emphasis which are social, educational and economic dimensions. NEPAD targets having African countries come up with home-based solutions to the various continental issues, for instance, illiteracy, diseases and poverty. Infrastructure, particularly, Information, Communication and Technology is cited as an important action area in the creation of favourable conditions for learning and sustaining development.[113] In order to fulfill the identified ICT aims, the NEPAD e-Africa commission was instituted and mandated to formulate and execute the NEPAD ICT initiative. Among the top priority programmes as highlighted by the commission is the NEPAD e-school initiative (or NEPAD ICT Pilot Schools Project). This

[111] African Union Commission. First Ten-Year Implementation Plan 2014 – 2023 of Agenda 2063. (Addis Ababa: African Union Commission, 2015), 16.
[112] Ibid.
[113] Gianluca C. Misuraca. *E-Governance in Africa, from Theory to Action: A Handbook for Local Governance*. (Ottawa: International Development Research Centre, 2007), iii

initiative involves several countries and numerous stakeholders and targets transferring ICT knowledge to both primary and secondary school students in Africa in order to lift education quality as well as availing information to the people's convenience.[114] It is termed as multi-stakeholder since it engages various private organizations within the ICT sphere willing to cooperate with participating countries.

The incorporation of information systems in the academic system has enabled provision of alternative strategies to the challenges experienced in the mainstream educational system. It has also enabled a wider reach of knowledge notwithstanding the limited resources in African countries. The development of learning technologies particularly provides a practical-oriented and easily accessible and comprehensive learning environment. The ongoing digital revolution in Africa has occasioned increase in trials on the use of ICT in education, both within and outside the classroom.[115] ICT has been utilized in various learning institutions and it has helped the learners to undertake comprehensive research thereby equipping them with adequate information concerning their line of study. The application of information systems has also led to a tremendous reduction in illiteracy levels among Africans as they have become more exposed to the outside world by being connected to the internet where they get educated in different ways.[116] This essentially helps in terms of transformation of the way the people think and their perception of issues. For example, the availability of cell phone technology in Niger influenced illiterate

[114] Gianluca C. Misuraca. *E-Governance in Africa, from Theory to Action: A Handbook for Local Governance*. (Ottawa: International Development Research Centre, 2007), iii

[115] Rohen d'Aiglepierre et al. "*How Digital Technology Can Help Re-Invent Basic Education in Africa*." Quartz Africa Journal, November 13, 2017

[116] Ibid.

traders to learn how to read and write purposely for drawing benefits from the lower costs of sending messages as compared to making phone calls.[117]

Information systems and infrastructure have also been extensively applied in enhancing the agricultural sector in Africa. The strategic employment of ICT on the agricultural sector, being the biggest sector in most African countries, offers an ideal opportunity for poverty reduction and economic development on the continent.[118] Many countries have embraced agriculture as a source of food security and also for the growth of their respective economies. Farmers use various information systems to access information regarding prices for their products from both national and global jurisdictions and also to connect with other farmers and agricultural policy makers and specialists. Systems, which include phone applications, have been instituted to assist farmers to remotely control their farm operations and in the monitoring of the activities and information about their crops remotely.

Application of ICT in weather forecasting has been applied widely across Africa and information concerning the weather is communicated through the mass media to the interested parties which helps farmers to plan farming activities and identify best crops to grow in a specific season depending on information on rain patterns in a particular span of time. [119] Information systems have greatly enabled meteorologists carry out these activities effectively and it has also increased reliability of the forecasts. This has also aided in the management of floods which are a common

[117] Simin Ghavifekr and W.A.W. Rosdy. *Teaching and Learning with Technology: Effectiveness of ICT Integration in Schools.* International Journal of Research in Education and Science (IJRES), 1(2), 2015, 177

[118] Enock Yonazi et al (eds). *Use of ICTs for Agriculture in Africa*. Joint Report By the African Development Bank, Korean Trust Fund, World Bank Pfizer Trust Fund and World Bank Africa Regional Department, 2012, 3.

[119] UNESCO. *E-Learning: Promoting Distance Education at the Secondary Level, 2005*. http://portal.unesco. org/en/ev.phpURL_ID=28751&URL_DO=DO_TOPIC&URL_SECTION=201.html.

feature among African countries and hence facilitating effective management or reduction of the effect of those floods.

In the health sector, ICT has been used to boost quality of services in the health centers and also reduce health care cost and health information. It has also been applied in provision of health education, capacity development and enhancement of health research. ICT has also made important contribution in public health, as illustrated by the important part played by telemetry information in the management of onchocerciasis in West Africa as well as the internet application in the management of Severe Acute Respiratory Syndrome (SARS) outbreak.[120] Based on a study conducted in 2011 on the effect of ICT on the delivery of primary health services in Nigeria, specifically the Niger Delta, Sylvester Anie (2011) concluded that ICT has positively influenced rural dwellers in relation to primary health care services and that ICT was an indispensable element for effective provision of primary health care services in the region.[121] In particular, ICT is considered a bridge that aids the rural dwellers to traverse from the ancient times to a new enlightenment era in form of enhancement of awareness on control and prevention of endemic ailments, child and maternal health encompassing family planning, basic sanitation, appropriate treatment of injuries and common diseases, provision of important medication and immunization against major infectious diseases.[122] In remote locations in Sub-Saharan Africa that are characterized by poor communication networks, the advent of mobile phone devices, instant text messaging system and multi-media messaging modules has

[120] S. Yunkap Kwankam, *"What E-Health Can Offer,"* Bulletin of the World Health Organization, Volume 82, Issue No. 10 (2004), 800.
[121] Sylvester O. Anie, *"Impact of Information Computer Technology on Primary Health Care Services to Rural Communities in Niger Delta Region of Nigeria*," Library Philosophy and Practice, 2011, http://www.questiaschool.com/read/1G1-260691387/impact-of-information-computer-technology-on-primary.
[122] Ibid.

alleviated delays in relaying critical decisions.[123] In the case of Kenya, telemedicine has been introduced to provide health service through science and technology whereby a doctor in distant location can consult with a patient [124] Telemedicine thus allows physicians and healthcare facilities to grow their reach beyond their own offices. Advanced medical care such as cancer treatment centers has also been attained through science and technology. In child health, science and technology supports neonatal screening for diseases such as sickle cell anemia.

Civil engagement of individuals has also been made possible by the new forms of technology including social media and social networking, which provide an avenue for its users to seek for attention on issues which require action. Social media has also assisted in solving problems and reporting criminal activities which affect the well-being of African people. Further, information systems have enabled e-government action plans where the government strengthens its citizens relation, improve efficiency in delivery of services to its citizens, efficient deployment of public resources and also in the enhancement of international cooperation.

2.3 EMERGING PERSPECTIVES

The world economy is experiencing transformation in technological and market settings which could affect the position of Africa including its involvement on the global market.[125] Currently, many organizations are employing computer technology and computer literacy is often

[123] Tyler, M., Hughes, J., & Renfrew, H. (1999). Kenya: Facing the challenges of an open economy. In E.M. Noam (Ed.), Telecommunications in Africa (pp. 79-112). UK: Oxford University Press.
[124] Shikuku Shituma. *Adoption of Telemedicine in Hospitals in Nairobi County*. Research Paper Presented at the School of Business, University of Nairobi, November, 2013, 3
[125] Samuel M. Wangwe, ed., *Exporting Africa: Technology, Trade, and Industrialization in Sub-Saharan Africa* (New York: Routledge, 1995), 52

considered a necessary condition before being offered employment opportunities in the formal sector. The consequence of technological, socioeconomic and demographic disruptions on business designs will be felt in changes to the employment landscape.[126] This is largely due to the reduction in manual work which is being replaced by automation. Official information regarding the operations of organizations is increasingly being stored electronically and in order for an employee to retrieve such information, the employee must have some basic skills on how to operate a computer device.

In Africa, most of the universities and other learning institutions have limited books and other related sources of information. This limitation has, nevertheless, been resolved through the integration of electronic books in the institution libraries where the students can access them from distant locations. This has proved to be not only a cost effective yet efficient option in accessing reading materials but has also diminished the need for construction of huge library facilities to serve the rising student population in learning institutions.

Remarkable transformation has also been experienced in the telecommunications sector where individual entities have increasingly adopted the use of automated telecommunication services like electronic mails. This has in effect enhanced communication and operational efficiency in different sectors including the corporate world. According to Bella Mody et al (1995), for developing countries, such as African countries, effective provision of telecommunication services is a necessary condition for the development of strong market economies and that today, the importance of core enterprises and social undertakings for instance financial transactions,

[126] World Economic Forum. *The Future of Jobs and Skills*. (Geneva: World Economic Forum, 2016), 6

health services, information services, transport, and the education sector, are heavily reliant on the adequacies of the telecommunication infrastructure and services.[127]

Further, information systems are being employed in the provision of fundamental amenities and in delivering public services across several African countries. The Fifth African Governance Forum held in Maputo, Mozambique, in 2002 highlighted local level development as a vital aspect of good governance included being the use of ICTs.[128] The employment of technology at grassroots level has in turn continued to contribute towards improved quality of life of citizens of the concerned states. Examples to this effect include the automation of telecommunication in Gambia, the automation of expenditure checking system in Ghana, the road planning and safety system in Nigeria and the decentralized 'Huduma' public service delivery centres in Kenya. It is thus incumbent upon African states to fully utilize opportunities presented by information technology in order to make Africa a better place to live in. As pointed out in the Global Information Technology Report, 2015, it is not the connectivity aspect of information technology or the connectivity numbers that generate the worth, but rather the results realized from the connectivity.[129]

2.4 IMPACT OF INFORMATION SYSTEM ON DEVELOPMENT IN AFRICA

Advancement in information systems has triggered massive transformation in Africa. Technological devices such as mobile phones have revolutionized communication in Africa over

[127] Bella Mody, Johannes M. Bauer, and Joseph D. Straubhaar, eds., *Telecommunications Politics: Ownership and Control of the Information Highway in Developing Countries* (Mahwah, NJ: Lawrence Erlbaum Associates, 1995), viii

[128] Gianluca C. Misuraca, *E-Governance in Africa, from Theory to Action: A Handbook on ICTs for Local Governance* (Ottawa: International Development Research Centre, 2007), 3

[129] Soumittra Dutta et al (eds). Global Information Technology Report, 2015 (Geneva, World Economic Forum, 2015), ix

the past decades and almost every home has accessibility to mobile phones which has made communication even much easier and reliable.[130] These mobile phones have provided millions of jobs across Africa which has also led to increased government earnings in form of revenue collected from the mobile phone vendors and other related service providers. The World Bank report for 2007 indicated that between the year 1995 and the year 2007, Africa registered positive economic growth,[131] partly attributable to automation of business processes. The report further showed that fourty-six Sub-Saharan countries introduced at least one business environment reform over the previous year and that Ghana and Kenya were ranked among the world's top ten reformers globally in 2006/07.[132]

Development of the IT sector has also inspired the lives of Africans, driven entrepreneurship, innovation as well as income growth. Elena Kvochko (2013) observes that ICT constitutes some of the rapidly developing industries that create numerous job opportunities directly and that it is also a critical development and innovation enabler.[133] Technology has transformed the business sphere in Africa dramatically.[134] This is evident in countries such as Kenya where mobile phones are used to transact businesses and make payments, augment filing of tax returns by citizens, among other contributions. These transactions have for instance been realized through the MPESA automated mobile phone money transfer platform. The IT sector has also led to greater heights of transparency and openness resulting from enhanced interaction and sharing of information and shaping of public opinion via social media platform. Indeed, the challenge posed

[130] UNESCO. *e-Project ABC - Mobiles for Literacy*. Background Case Study authored for UNESCO by Christopher Ksoll in 2013. [Unpublished].
[131] World Bank. *African Development Indicators*, (Washington, The World Bank,2007), 1
[132] Ibid., 3
[133] Elena Kvochko. *Five Ways Technology Can Help the Economy*, World Economic Forum, 2013, https://www.weforum.org/agenda/2013/04/five-ways-technology-can-help-the-economy/
[134] Serianu Research Team. Africa Cyber Security Report (Nairobi: Serianu Limited, 2016), 11

on African countries borders on continued understanding of technological changes as a basis for developing the capacity to respond constructively and positively.[135]

2.5 INFORMATION SECURITY TRENDS IN AFRICA

Internet connectivity in Africa is on the rise and dependence on internet amongst African states has sharply increased. [136] The growing social and economic dependency on ICT has over time brought new challenges and the need for a resilient and robust infrastructure. As more corporate entities digitize their processes and move to the internet, the potential attack agents for these entities expand.[137] In this regard, protection of information assets is a priority concern and cyber security and data protection issues are at the apex of Africa's security interventions. Effective information security intervention calls for all stakeholders within the African internet ecosystem to work in collaboration so as to achieve the protection of the interconnected internet infrastructure and also preserve all the fundamental rights and properties of the internet. [138]

In the year 2014, the African Union adopted the African Union Convention on Cyber Security and Personal Information Protection and to enable implementation of Convention terms, the AU Commission requested the Internet Society to join hands with the Commission in the development of internet infrastructure guidelines for the African continent.[139] Both global and international internet experts collaborated with government representatives and other important stakeholders including network operators in formulating these guidelines.

---

[135] Samuel M. Wangwe, ed., *Exporting Africa: Technology, Trade, and Industrialization in Sub-Saharan Africa* (New York: Routledge, 1995), 52

[136] Internet Society. Internet Infrastructure Security Guidelines for Africa. https://www.internetsociety.org/resources/doc/2017/internet-infrastructure-security-guidelines-for-africa/#_ftn1

[137] Serianu Research Team. Africa Cyber Security Report (Nairobi: Serianu Limited, 2016), 11

[138] Internet Society. op.cit.

[139] Ibid.

The guidelines largely underscore the importance of adopting a multi-stakeholder structure and a synergetic security strategy in the protection of Africa's internet infrastructure. [140] They emphasize four vital components regarding data security which are; awareness, responsibility, cooperation and adherence to internet properties and other fundamental rights regarding information security. They also recommended specific actions by the various stakeholders on the internet infrastructural security landscape. This approach was attributed to the African cyber security features which include limited number of skilled human resources, limited financial resources to enable organizations and governments in the allocation of enough funds towards cyber security, low level of awareness on cyber security related issues among the Africans and finally, inadequate know-how concerning the risks involved in the use of ICTs.[141]

At regional level, a committee was formed and entrusted in the advisory of policy makers on capacity building and regional strategies and also to facilitate information sharing across the continent. At national level, governments are supposed to take service based methodologies in the identification of critical information security infrastructure for protection purposes, develop multi-stakeholders structures for advising the public and organizations concerning cyber security strategies and policies so as to facilitate the process of information sharing, promote the use of internet exchange points as well as greater connectivity involving different networks within the continent so as to foster resilience of internet infrastructure. Governments are also expected to adopt and follow best practices of cyber security within their infrastructure and institutions and promote the same amongst stakeholders.

[140] Internet Society. Internet Infrastructure Security Guidelines for Africa. https://www.internetsociety.org/resources/doc/2017/internet-infrastructure-security-guidelines-for-africa/#_ftn1
[141] Ibid.

At operational level, baseline security should be established through the execution of vital channeling and domain name system security strategies, network security and other important practices in order to scale up production of a clear and a positive transformation of the internet infrastructure in Africa.[142] This responsibility should be undertaken in a collaborative arrangement by network providers and other service agents. At organizational level, organizations are to implement the best and current practices and also strive to create a cyber-security culture at all levels. This implies from top management all the way to the junior employees. Article 21 of the Convention document provides for security obligations where it is stated that data controllers amongst the AU member states must take all appropriate precautions, according to the type of data, and in particular, to prevent such data from being accessed or altered or destroyed by unauthorized third parties.[143] Three major components exist, that is, area security, people security and data security. Area security encompasses the physical safety of the space which is inclusive of physical accessibility controls. Securing facilities and premises, working in safe environment and loading and delivery zones are important elements of area security. Equipment security involves managing siting and protection of equipment, capability security, power supply, safety of organizational equipment that are not within the premises, equipment maintenance and secure disposal or recycling of the equipment. It also entails the overall clear screen and clear desk policy controls and guidelines that encompass removal of property around the physical security area. The important principle is that every individual is liable as part of their official duties. Staff screening is instituted together with confidentiality

[142] Internet Society. Internet Infrastructure Security Guidelines for Africa. https://www.internetsociety.org/resources/doc/2017/internet-infrastructure-security-guidelines-for-africa/#_ftn1

[143] African Union Convention. *African Union Convention on Cyber Security and Personal Data Protection*, July, 2014, (Addis Ababa: African Union Commission, 2014), 23

accords and security responsibilities incorporated amongst the terms and conditions of service. End users ought to be equipped with adequate safety information and training.[144]

Information security comprises of a collection of policies, procedures, and technologies. Policy provisions and guidelines are the foundation of the manner in which security measures function and are inclusive of response to security incidents as observed above. This may differ markedly amongst different organizations. Policies and guidelines ought to be recorded for ease of reference and comprehension.[145] If a corporate entity's efforts on information security are engraved such that all emphasis is directed on the same output and outcome, then the management of information security must reside in a framework easily understood by all across the organization.[146] The technology involved in implementing data security is a mixture of services, software and hardware. Services are further classified into educational services, professional services and controlled security services. Educational services entail employee, contractor or even partner awareness training. Professional services involve aiding in designing policies, executing of policies, procuring appropriate technology, among others. Controlled security services entails delivery of a variety of security functions for a monthly fee.

To address emerging cyber security issues and provide strategic thrusts to Africa's efforts of enhancing its cyber security posture, a number of cyber security forums have also been organized across the African continent. These include the Africa Internet Summit that was launched in Gambia in 2012, the annual Internet Information Security Conference in

[144] Margaret Rouse. *Information Security*. http://searchsecurity.techtarget.com/definition/information-security-infosec (Accessed on March 15, 2018), 6
[145] Ibid.
[146] Qingxiong Ma et al., "An Integrated Framework for Information Security Management," *Review of Business Journal*, Vol. 30, Issue No. 1 (2009)

Johannesburg, Republic of South Africa and the 2018 Africa Cyber Defence Summit in Nairobi, Kenya. The convening of regional and continental internet security forums draws from the fact that cyber security violations and attacks are becoming incumbent impediments to Africa's transformation.[147] The deliberations are therefore aimed at consistent cyber security dialog for purposes of protecting sensitive data and critical information infrastructure.

2.6 GOAL OF INFORMATION SECURITY MANAGEMENT IN AFRICA

Africa currently hosts some of the most rapidly growing economies globally and the entire continent is set for a huge economic transformation.[148] Given the role of ICT in the growth trajectory, cyber security violations and attacks potentially slow down development. In this regard, information security management has become a critical component in the administration of the affairs of African states. In many instances, it is hard or almost impossible to transact business without smooth and proper functioning information systems.[149] In the words of Johnson et al (2014), regulation of information security is vital given that the internet has no boundaries, hence easily enabling international crimes as well as remote hacking.[150] In the African context, there is a felt need for public organizations to evaluate the entire security situation using a top-bottom strategy to determine requirements for data security.

[147] Naseba and Africa Cyberspace Network. *Africa Cyber Defence Summit*, https://www.eventbrite.com/e/africa-cyber-defence-summit-2018-nairobi-kenya-tickets-43780384308, (Accessed June 23, 2018)
[148] Ibid.
[149] M. Zviran and W.J. Haga. Password Security: An Empirical Study. Journal of Management Systems, Vol. 5, Issue No. 4, 1999, 162.
[150] Joseph Johnson et al., "A Comparison of International Information Security Regulations," *Interdisciplinary Journal of Information, Knowledge and Management* 9 (2014)

The objective of information security management is to present a timely, accurate and comprehensive image of the security status of an organization. This overview allows the organization to reduce the potential risk or interference with its activities and in the event of adversarial events or incidents, to mitigate consequences of such incidents on the organizational entity thereby enabling timely resumption of full operations.[151] According to Qingxiong et al (2009), data security management is a crucial component of the strategic plan of a successful organization.[152] Whilst the objectives of data security management may appear relatively simple to mention, the practical aspect is a totally different thing. This is attributed to the fact that the ICT infrastructure is becoming highly sophisticated. It is also as a result of increasing number and complexity of applications, increased accessibility to huge volumes of data by individuals and enterprises, rising intricacy of threats and advanced functionalities of adversaries. Data security architecture is heterogeneous in nature which implies that security sensor information is relayed in different languages and formats giving rise to new areas of vulnerability emanating from wireless equipment and local area networks.[153]

Information security management entails a collection of activities created courtesy of antiviruses, firewalls and antimalware data sensors as well as through vulnerability diagnostic input.[154] As observed earlier, an amalgamation of data security tasks ought to be carried out so as to reduce the potential risk from fused threats. A component of key concern on data security management relates to establishment of specific elements of the traffic that are relevant to the information security cycle. Management of incidents is, therefore, a continuous process that comprises of six

[151] Margaret Rouse. *Information Security*. http://searchsecurity.techtarget.com/definition/information-security-infosec (Accessed on March 15, 2018), 6.
[152] Qingxiong Ma et al., "An Integrated Framework for Information Security Management," *Review of Business Journal*, Vol. 30, Issue No. 1 (2009)
[153] Rouse. op.cit., 6
[154] Ibid., 11

stages, that is, preparation, identification, containment, eradication, recovery and documentation phases. The preparation phase entails laying the foundation and inventory of the IT infrastructure elements. Additionally, it requires, inter alia, instituting of priorities and standard operating protocols. Identification entails the affirmation of the form and specific incident type, whilst containment has to do with limiting the potential harm. Eradication simply means to remove the threat completely. Recovery involves restoration of functions and information to the previous state. Finally, documentation implies keeping records of every activity undertaken in the process.[155]

Information security management is a very important function in organizations with increased internet dependence as well as those with sophisticated IT infrastructure. The diversity of the ICT surroundings and data security infrastructure which aids them requires a significant level of focus as regulatory and organizational settings add to the pressure. According to Odedra, African countries should apply ICT selectively for particular and segregated use in order to gain noticeable advantages not only to their economies but also to the advancement of the welfare of its people.[156] Flexible and effective management of data security is central to business continuity. In fact big corporations with large numbers of users require to constantly keep themselves abreast of the state of security of their respective information assets at any given time. The idea of closed perimeter is fast fading and there is therefore a compelling need to deploy expedient security strategies to safeguard the highly dynamic business designs. The choices of application of information systems should match with that of the African Union and individual state priorities so as to have desired effect on development.

[155] Margaret Rouse. *Information Security*. http://searchsecurity.techtarget.com/definition/information-security-infosec (Accessed on March 15, 2018), 11

[156] Odedra, M. *Information Technology Transfer to Developing Countries: Cases from Kenya, Zambia and Zimbabwe*. PhD Thesis, London School of Economics, September 1990.

2.7 PRINCIPLES OF ISMS AND THEIR RELEVANCE TO AFRICA

While the implementation of ISMS varies amongst different organizations, there are fundamental principles that all ISMS must follow to effectively protect Africa's public sector information resources. The first basic principle for the successful administration of ISMS is having an objective and striving towards its realization. This objective should be focused towards instilling customer confidence, business continuity, business opportunity and investment promotion or reducing harm on the business landscape through prevention and minimizing the effects of security breaches.[157] An effective security program is a customized program whose attributes are dependent on the objective, resources as well as organizational operating environment.

The second fundamental principle of ISMS is aligning information security strategy with the organizational mandate or business strategy.[158] For an effective ISMS, an organization must assess the security requirements of each information resource and apply the appropriate controls to guarantee protection of those assets.[159] Alignment could be pursued by way of understanding institutional objectives by top IT planners, shared understanding between the top management and information security planners and an elevated status of data security function in the organization.[160] Not all information resources need the same controls and there is no panacea for information security. In the same context, institutional information arises in different shapes and sizes. Different control strategies are therefore required to keep the information secure.

[157] Qingxiong Ma et al., "An Integrated Framework for Information Security Management," *Review of Business Journal*, Vol. 30, Issue No. 1 (2009), 1

[158] Ibid.

[159] Perry Johnson Registrars Inc. *Information Security Management System*. http://www.pjr.com/standards/iso-27001/information-security-management-system (Accessed on March 24, 2018)

[160] B.H. Reich and I. Benbasat. *Factors that Influence the Social Dimension of Alignment Between Business and Information Technology Objectives*, MIS Quarterly Journal, Vol 24, Issue No. 1 (2000), 82

Thirdly, ISMS looks at an organization from the perspective of a work system which comprises of two interacting systems that are independent of each other, namely, technical system and social system.[161] The technical system is concerned with the functions, methodology and technology required to translate inputs into outputs. The social system focuses on characteristics of individuals, for examples, education and skills, values, relationships amongst the people, authority structure and reward system.[162] The output of the work system accordingly arises from the joint interaction of the two systems. Whereas there are many technical aspects to the creation of an ISMS, a crucial aspect of ISMS falls within the management domain. One identified weak link to information security is that of employee, the person who accesses or verifies critical information every day. According to Francis Waithaka (2018), insider threats top the list of high risks and the most implicated group is that of administrators and other privileged users, who are better placed to institute malicious breach, and whose acts of negligence or mistakes could cause considerable damage to the organization.[163] In this regard, an ISMS ought to encompass policies and protocols that safeguard an organization from the misuse of data by employees. These guidelines must have the support and supervision of the management to be effective. Besides formal policies and processes, the management is also expected to influence an organization's culture to reflect the value placed on security of information. An organization should particularly sensitize key stakeholders of the necessity of information security.[164] Without the participation of people who implement, supervise or maintain an ISMS, it will be hard to achieve and maintain

[161] R. Bostrom and J. Heinen. *Management Information System Problems and Failures: A Socio-Technical Perspective*. MIS Quartely Journal, September, 1977, 14

[162] Qingxiong Ma et al., "An Integrated Framework for Information Security Management," *Review of Business Journal*, Vol. 30, Issue No. 1 (2009)

[163] Francis Waithaka. *Insights from Africa Cyber Security Report*. https://digital4africa.com/2018/04/20/insights-africas-cyber-security-report/ (Accessed June 23, 2018)

[164] Perry Johnson Registrars Inc. *Information Security Management System*. http://www.pjr.com/standards/iso-27001/information-security-management-system (Accessed on March 24, 2018)

the level of assistance required to create and maintain a certified ISMS. Whereas this is not easy, it is core for effective implementation of ISMS.

Lastly, ISMS implementation is dynamic. To guarantee organizational security from threats to information assets, an ISMS must consistently expand and evolve to adapt to the changing technical landscape. In the ISMS cycle, new forms of vulnerabilities against systems applications and infrastructure components are discovered virtually on a daily basis, thus necessitating continuous endeavour by security officials to remain updated on emerging information security threats and instruments.[165] In this regard, continuous re-evaluation of the ISMS is essential. By regular testing and assessment of ISMS, an organization will establish whether its information is still safeguarded or if adjustments need to be made.[166] Just as organizations adjust to variations in business environments, ISMS also need to change accordingly to advances in technology and new organizational information.[167]

The above principles can be employed by Africa public sector organizations in managing risk dynamics within the organizations' managerial and business processes. They could particularly assist African states in ensuring that public sector management processes take into account not only the broad objectives, but also information security requirements with specific focus on structure and unique organization attributes. This is useful for a corporate entity that reorganizes its core business in order to better manage changes in risks related to today's organizational processes.

[165] Qingxiong Ma et al., "An Integrated Framework for Information Security Management," *Review of Business Journal*, Vol. 30, Issue No. 1 (2009)
[166] Perry Johnson Registrars Inc. *Information Security Management System*. http://www.pjr.com/standards/iso-27001/information-security-management-system (Accessed on March 24, 2018).
[167] Ibid.

2.8 APPROACHES FOR THE IMPLEMENTATION OF ISMS IN AFRICA

The dynamic Information Technology (IT) trends have resulted in organizations using different approaches in managing information security.[168] To deter attackers and mitigate organizational vulnerabilities at various points, there are thus multiple security controls that are available for use by African states as part of layered defense strategy. This would in essence allow organizations to contain and restrict the damage, eliminate the cause and execute updated defense controls.[169] Agosa (2014), identifies three key ISM practices as the Information Technology Infrastructure Library (ITIL), Control Objectives for Information and related Technology (COBIT) and ISO/IEC 27000 series.[170] These practices underpin different aspects and conditions necessary for the realization of both organization and business goals.

ITIL emphasizes vital business procedures and disciplines required to deliver quality services.[171] It classifies all business activities under two categories of service delivery and service management. This strategy looks at ICT quality based on the degree of alignment of ICT services alongside concrete business requirements.[172] According to Jean-Pierre Garbani (2005), ITIL describes the procedures to be adopted in the delivery and support of IT services with strong emphasis on the business. The ITIL philosophy is centred on the service counter as a communication

[168] Madiavale Beverly Agosa. *Information Security Management Practices and Organizational Goals: A Study of Microfinance Organizations In Nairobi*, Research Paper, University of Nairobi, October 2014, 2

[169] Margaret Rouse. *Information Security*. http://searchsecurity.techtarget.com/definition/information-security-infosec (Accessed on March 15, 2018)

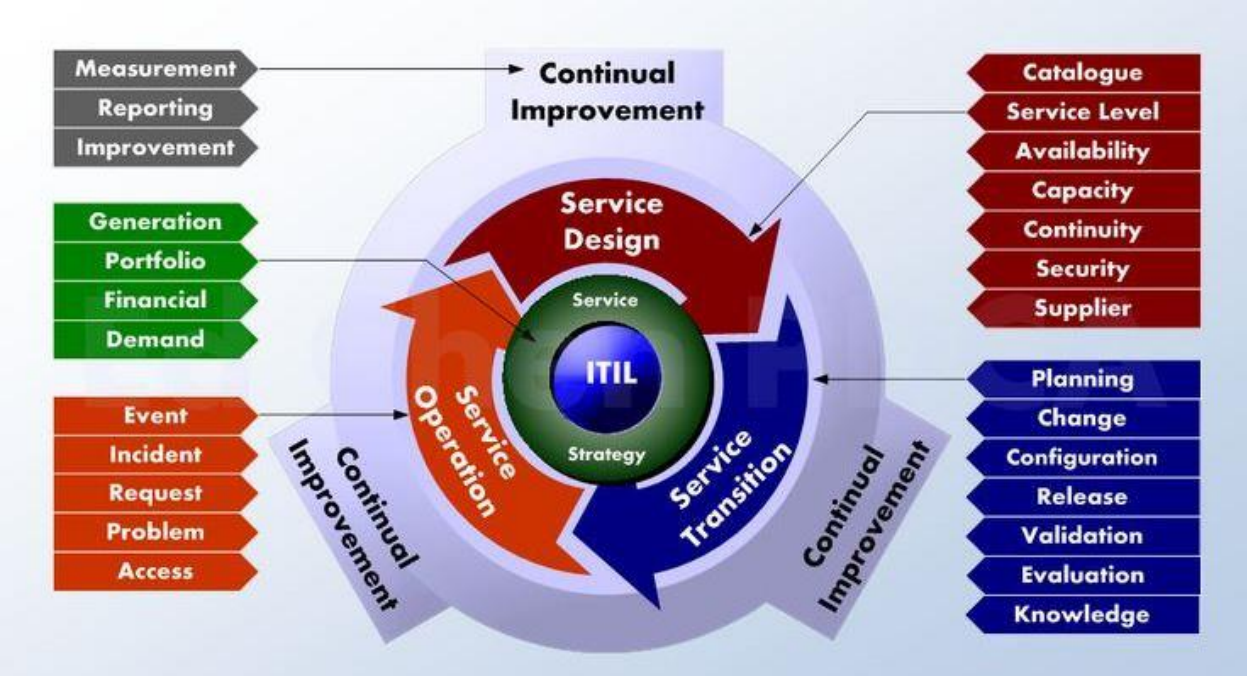
[170] Agosa. op.cit., 2.

[171] Ibid., 3

[172] H.M. Larsen, K.M. Pedersen and K.V. Andersen. *"IT Governance Reviewing 17 IT Governance Tools and Analysing the Case of Novozymes"* .Proceedings of the 39th Hawaii International Conference on Systems Science, 2006.

podium and the configuration management database (CMDB).[173] ITIL is strong on delivery and support processes and vividly defines ways of structuring operational procedures. It is, nevertheless, weak on security procedures and controls.[174] A graphical presentation of the ITIL model is given below.

Figure 1: ITIL Lifecycle



SOURCE: Mark Bryant, Pinterest Social Network

COBIT's main focus is on development of clear guidelines and appropriate IT security and control practices. It provides managers with an array of globally acceptable actions, processes, identifiers and ideal strategies to assist in magnifying merits sourced via incorporation of IT and

[173] Jean-Pierre Garbani. *ISO, ITIL, COBIT: The Management Process*, CSO Journal, October 4, 2005 on https://www.csoonline.com/article/2119437/data-protection/iso--itil--cobit--the-management-process-alphabet-soup.html

[174] Ibid.

formulating apt ICT control and governance infrastructure in an organization.[175] COBIT consolidates an up-to-date universally accepted control toolss for use by ICT managers and business executives. It tackles critical operational and IT governance issues regarding process improvement.[176] According to Jean-Pierre Garbani, (2005), COBIT emphasizes on governance, controls and metrics. He further observes that COBIT lacks security elements but offers a more global perspective of IT procedures at the IT structure management conditions than ITIL.[177]

ISO/IEC is an information security framework that offers a wide-ranging collection of controls and ideal practices.[178] This standard provides a single reference point for identification of appropriate controls for situations where information systems are deployed in industry and commerce.[179] The standard prescribes a global approach to management of security that outlines responsibilities and establishments tasked with security and policies, critical asset classification and risk management.[180] According to Indian Register Quality System, the ISO / IEC 27001 is the only verifiable international standard that defines conditions for an ISMS.[181] The standard is structured to assure selection of appropriate and proportional security controls.

This study, accordingly, directs greater focus on the ISO/IEC 27001 ISMS standard.

---

[175] Madiavale Beverly Agosa. *Information Security Management Practices and Organizational Goals: A Study of Microfinance Organizations In Nairobi*, Research Paper, University of Nairobi, October 2014, 2

[176] Jean-Pierre Garbani. *ISO, ITIL, COBIT: The Management Process*, CSO Journal, October 4, 2005 on https://www.csoonline.com/article/2119437/data-protection/iso--itil--cobit--the-management-process-alphabet-soup.html

[177] Ibid.

[178] Agosa, op.cit, 2

[179] H.M. Larsen, K.M. Pedersen and K.V. Andersen. *"IT Governance Reviewing 17 IT Governance Tools and Analysing the Case of Novozymes"* .Proceedings of the 39th Hawaii International Conference on Systems Science, 2006.

[180] Jean-Pierre Garbani. *ISO, ITIL, COBIT: The Management Process*, CSO Journal, October 4, 2005 on https://www.csoonline.com/article/2119437/data-protection/iso--itil--cobit--the-management-process-alphabet-soup.html

[181] Indian Register Quality System. *Information Security Management System.* http://www.irqs.co.in/information-security-management-system.html (Accessed on February 15, 2018)

2.8.1 Overview of ISO and ISO Standard on ISMS

The International Organization for Standardization (ISO) is an independent, non-governmental international body that comprises of 162 national standards entities. The organization was established in 1947 and is a global leader in development of voluntary international standards thereby facilitating global business by way of providing common standards applicable amongst different countries of the world.[182] The organization brings together experts for purposes of sharing knowledge and experience and developing international standards that are market oriented and consensus-based and that that enhance innovation as well as providing solutions to global challenges. These standards consequently provide a stage for developing practical tools based on common understanding and collaboration with all stakeholders.[183] The activities of the organization are centrally coordinated by a Secretariat situated in Geneva, Switzerland. Arising from its international network, ISO members are drawn from every corner of the world. The organization operates in collaboration with over 700 institutions and in excess of 100,000 experts from various sectors and industries. These include the International Telecommunication Union (ITU), the International Electro-technical Commission (IEC) and the World Trade Organization (WTO) where a strategic partnership has been struck aimed at promoting free and fair trade.[184] The ISO brand is thus recognized globally and associated with confidence.

An International Standard is basically a document containing practical information bordering on best practices. Normally, it defines an agreed mode of operation or remedy to a global challenge.

[182] International Organization for Standardization. *All About ISO*. https://www.iso.org/about-us.html (Accessed on March 20, 2018)
[183] International Organization for Standardization. *ISO in Brief*. (Geneva: ISO Central Secretariat, 2016), 2
[184] Ibid., 9

International Standards provide world-class description for products, systems and services to ensure safety, quality and efficiency. The ISO has so far published about 22026 International Standards and related documents, reaching out to almost every industry, from agriculture, to healthcare and technology.[185] The popular standards include ISO 9001 on Quality Management, ISO/IEC 27001 on Information Security Management, ISO 14001 on Environmental Management, ISO 22000 on Food Safety Management and ISO 50001 on Energy Management.

The ISO 9000 series refers to a set of five International Standards for Quality Assurance. It contains not rules, but a set of conditions that organize their processes and make organizations more cost effective.[186] The ISO/IEC 27000 series on the other hand relates to information technology security techniques and it, among others, provides features considered essential for managing information assets.[187] According to Janshcob and Tsinstifa (2006), ISO/IEC 27000 series of standards specifies requirements in designing and implementing an appropriate ISMS in the organization ensuring that adequate and appropriate controls are instituted to safeguard information resources thereby enhancing stakeholder confidence.[188] The series encompasses about twenty standards where the first three, ISO/IEC 27000, ISO/IEC 27001 and ISO/IEC 27002 define the vocabulary, code of practice and requirements, respectively, while the other standards in the series offer general guidelines for, among others, management of security threats, quantification, auditing as well as sector specific guidelines.[189] ISO/IEC 27001 is thus part of the ISO/IEC 27000 group of standards that provides specification and sets out general

[185] International Organization for Standardization. *ISO in Brief*. (Geneva: ISO Central Secretariat, 2016), 3
[186] ISO Certification. https://www.isoeasy.org (Accessed on March 14, 2018)
[187] Lois Evans, "Protecting Information Assets Using ISO/IEC Security Standards," *Information Management*, November-December 2016
[188] Angelika Jaschob and Lydia Tsintsifa. IT-Grundschutz: Two-Tier Risk Assessment for a Higher Efficiency in IT Security Management. Information Security Solution Europe Conference, Rome, Italy, 2006, 95
[189] Evans, op.cit

requirements for ISMS.[190] The standard is issued by ISO and IEC under a joint initiative.[191] It comprises eleven security domains and is concerned with security compliance at all levels. These domains include Security Policy, Data Security Organization, Asset Management, Environmental and Physical Security, Human Resources Security, Acquisition of Information Systems, Communication and Operations Management, Data Security Incident Management, Access Control, Business Continuity Management, Development and Maintenance and Adherence. The standard aims to guarantee the choice of appropriate security tools to safeguard information resources. The standard is applicable to all forms of organizations either public or private.

The ISO/IEC 27001:2013 standard is amongst the latest updates of internationally acclaimed practice code for managing data security within the ISO/IEC 27001 classification category. It focuses on controls that organizations ought to implement to ensure they manage risks relating to safeguarding information and information infrastructure resources in a reasonable manner.[192] This standard aims to provide a reference point for identifying necessary controls in situations where information systems are being used.[193] It postulates the conditions for setting up, implementing, sustaining and continuously improving an organization's ISMS. It basically describes what organizations should do to establish and implement an ISMS and not how to do it. The standard defines a set of information security management requirements as defined

[190] M.B. Agosa. *Information Security Management Practices and Organizational Goals: A Study of Microfinance Organizations in Nairobi*. Research Project. Nairobi, 2014.
[191] International Organization for Standardization. "ISO - ISO Standards - ISO/IEC JTC 1/SC 27 - IT Security Techniques".On https://www.iso.org/committee/45306/x/catalogue/
[192] J. Owiti. "*Information Security Management Present and Future*". ICPAK 27th Annual Seminar, 2011.
[193] H.M. Larsen, K.M. Pedersen and K. V. Andersen. "*IT Governance: Reviewing 17 IT Governance tools and Analyzing The Case of Novozymes A/S*" .Proceedings of the 39th Hawaii International Conference on Systems Science, 2006.

under seven segments, namely, Leadership, Planning, Context, Leadership, Operation, Assessment and Continuous Improvement.[194]

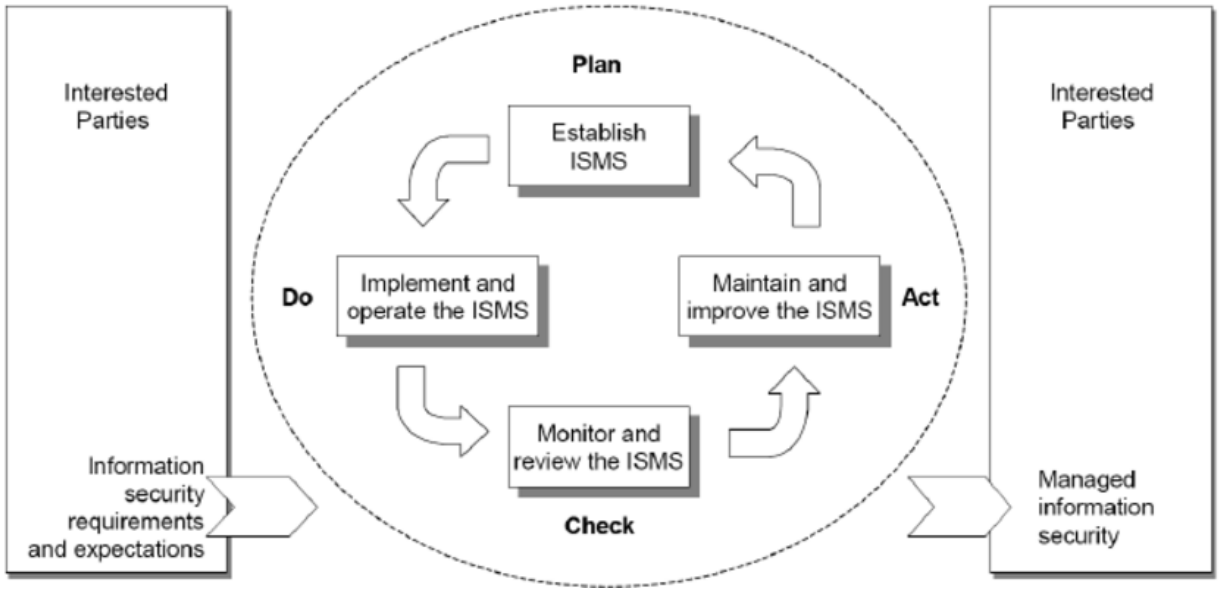
The ISO standard could be used to gauge an organization's ability to accomplish information security obligations. It can be employed internally as criterion for assessing the organization's capability to meet its information security requirements through performance evaluation and internal audits. According to Amir Hormozi, the standard is applied internationally for quality administration and quality assurance.[195] It can also be employed by third parties as criteria for assessing capacity, which are known as second-party audits or third-party audits.[196] The standard uses a process methodology in the establishment, implementation, operationalization, monitoring, verification, sustenance and improvement of an organization's ISMS. Any activity that uses and manages resources to enable conversion of inputs to products is considered a process. Generally, the output arising from individual processes constitute inputs into the consequent processes. The process approach towards information security management encourages users to recognize the significance of comprehending organizational information security needs and defining corporate policies and data security objectives; establishing controls to govern the security risks of information relating to the general business risks of the organization; keeping track and evaluating the performance level and ISMS efficacy and continuous improvement based on objective considerations.

[194] International Organization for Standardization ISO/IEC 27001 International Standard.
[195] Amir M. Hormozi, "Understanding and Implementing ISO 9000: A Manager's Guide," *SAM Advanced Management Journal* 60, No. 4 (1995)
[196] International Organization for Standardization. op.cit.

The standard specifies conditions for creating and sustaining an ISMS in the setting of global business risks of the organization.[197] The ISMS procedures are premised on the Plan-Do-Check-Act (PDCA) model. Under this model, the concept Plan represents the establishment of ISMS. It entails establishing ISMS policy, aims, processes and strategies for managing threats and improving information security to achieve outcomes aligned with the overall organizational objectives and policies. Do relates to Implementing and Operating the ISMS. In particular, it is concerned with implementing and making use of the ISMS policy, processes, procedures and controls. Check refers to overseeing and evaluating the ISMS and it encompasses evaluating and, where appropriate, measuring the performance in regard to the ISMS policy, practical experience and objectives and reporting the results to the management. [198] Finally, Act has to do with maintaining and improving the ISMS and more specifically taking mitigation and corrective measures as informed by results of internal audit of the ISMS or other applicable sources of information to realize continuous improvement of the ISMS. Under this framework, therefore, quality undertakings ought to be planned, recorded and managed under specific environmental conditions.[199]

[197] International Organization for Standardization ISO/IEC 27001 International Standard.
[198] Ibid.
[199] William M. Lankford, "ISO 9000: Understanding the Basics," *Review of Business* Volume 21, Issue No. 1 (2000)

Figure 2: The PCDA Model



SOURCE: OECD Guidelines

Figure 2 above reflects a summary of the guiding principles of the PDCA model as spelt out in OECD Guidelines for Multinational Enterprises. It specifically offers a framework for fulfilling the conditions within the guidelines governing risk assessment, security design and implementation, security management and reevaluation.[200] The structure and execution of an entity's ISMS is shaped by its goals, security needs, processes used and structure and institution size. The level of implementation is grounded on the scope and needs of the organization.

[200] Organization for Economic Cooperation and Development. *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*. (Paris: OECD, July, 2002), www.oecd.org

2.8.2 General Requirements of the ISO Information Security Standard

ISMS is an organized way of managing an organization's information for security purposes.[201] It is a systematic business risk centered management practice that embraces people, IT systems and processes in ensuring information security of a corporate entity.[202] Important aspects of the ISO ISMS standard are explained below.

2.8.2.1 Establishing the System

To establish an ISMS, an organization must, among others, define the range and ISMS limits encompassing details and justifications for possible exclusions; define ISMS policy with reference to business type, location, resources and technology; define the organization's risk assessment approach; identify, analyze and evaluate risks; identify and assess risk treatment options and choose risk management objectives and controls.[203]

2.8.2.2 Implementing and Operating

In implementing and operating an ISMS, an organization is expected to, inter alia, create a risk treatment strategy that highlights appropriate administrative action, responsibilities, assets and areas of emphasis in handling data security threats; execute the plan so as to realize outlined control objectives, including funding considerations and assignment of tasks and obligations; apply selected controls to achieve control objectives; define ways of gauging the resourcefulness

[201] Indian Register Quality System. *Information Security Management System*. http://www.irqs.co.in/information-security-management-system.html (Accessed on February 15, 2018)
[202] Ibid.
[203] International Organization for Standardization. ISO/IEC 27001 International Standard.

of the designated controls and state how these measures will be employed to evaluate the efficacy of these controls to generate comparable results; implement capacity development and awareness creation programmes and implement measures and other controls that allow rapid security events detection and timely response to security incidents. Top leadership is expected to actively back security management within the organizational entity through provision of clear policy direction, demonstration of commitment, recognition of information security responsibilities and explicit assignment of duties. Information security undertakings should be coordinated by representatives of various organization parts with relevant responsibilities and job function.[204]

2.8.2.3 Monitoring and Reviewing

An organization is expected to carry out monitoring and verification operations and related checks, ensure frequent ISMS effectiveness appraisals (including compliance with ISMS guidelines and targets and security control reviews), putting into consideration output of security audits, incidents reports, comments and suggestions of stakeholders and measurement of usefulness of controls to verify level of compliance with safety requirements.[205] In the words of Lois Evans (2016), organizations must determine what is monitored and measured and when and how results should be analyzed and evaluated.[206] In addition, organizations are expected to conduct risk evaluation at preplanned ranges, undertake analysis of residual threats and isolate tolerable risks, perform in-house ISMS audits at regular intervals, periodically review ISMS

[204] International Organization for Standardization. ISO/IEC 27001 International Standard.
[205] Ibid.
[206] Lois Evans, "Protecting Information Assets Using ISO/IEC Security Standards," *Information Management*, November-December 2016

management to ensure the scope remains acceptable and update the security plans to reflect the results of oversight and audit activities.

2.8.2.4 Maintaining and Improving

Under this category, organizations ought to implement ISMS improvements, undertake applicable mitigation and corrective activities and utilize lessons derived from the safety experiences of the entity and other organizations. An ISMS must thus exist in an atmosphere of continual improvement.[207] Organizations are also expected to relay the enhancements or other related undertaking pursued by all interested groups with some degree of precision commensurate to the prevailing conditions and map out the way forward besides ensuring that the improvements realize intended objectives.[208]

2.8.2.5 Documentation Requirements

ISMS documentation includes maintenance of management decision records, ensuring any action taken is traced back to resolutions and policy prescription made by management and also ensuring that registered results can be reproduced. [209] It is essential for an entity to be in a position to exhibit the link between specific restrictions and outcomes of threat management protocols and ultimately to the ISMS objectives and guidelines.

[207] Lois Evans, "Protecting Information Assets Using ISO/IEC Security Standards," *Information Management*, November-December 2016
[208] International Organization for Standardization. ISO/IEC 27001 International Standard.
[209] Ibid.

Documentation of ISMS ought to specifically incorporate documented ISMS objectives and policy statements, the ISMS scope, controls and procedures that support the ISMS, a concise depiction of the risk evaluation procedure, a threat evaluation report, a risk mitigation and treatment plan, recorded intervention measures of the institutional entity to guarantee successful planning, running and regulation of its data security processes as well as description of the manner of quantifying the efficacy of controls, documents required by the global standards and the applicability statement.

2.8.2.6 Internal Audits

Organizations are expected to perform ISMS internal audits at scheduled timelines to establish whether the goals, processes, procedures and controls of the instituted ISMS conform to the standard requirements and applicable laws or regulations, comply with highlighted data security conditions, are successfully executed and sustained and also whether they deliver the desired results. [210] An audit undertaking should be prearranged with keen emphasis on the significance and existing status of the various processes, different areas of monitoring and the outcomes of preceding audits. Besides, the audit criterion, scope, frequency and approaches must be defined. The choice of ISMS auditors as well as audit procedure should guarantee fairness and unbiased opinion. Auditors are in this regard not expected to carry out audit of their respective areas of work.

[210] International Organization for Standardization. ISO/IEC 27001 International Standard.

The requirements and responsibilities for preparing and executing ISMS audits, communicating audit results and record keeping, must be indicated in a well-documented procedure.[211] The individual in charge of the section being audited is expected to ensure that timely action is taken to eliminate both identified nonconformities and the causes. Follow-up action encompasses verification of measures pursued and conveyance of results. It also entails efforts to detect potential non-conformities before they occur.[212]

2.8.3 Scope of the ISO/IEC 27001:2013 ISMS Standard

ISMS is a set of correlated tools used by organizations to control and manage information security threats and to safeguard and sustain the integrity, confidentiality and availability of information. These tools comprise roles, practices, plans, procedures, policies, processes, resources, structures and responsibilities that are employed in managing security threats and safeguarding information. The modalities of implementing the ISMS standard depend on institutional objectives, prevailing data security risk portfolio and requirements as well as stakeholder expectations. It is also shaped by the intrinsic complexities associated with a corporate entity including the corporate setting. The specific way of employing the standard is dependent on the institution's distinct structure, the regulatory, legal and contractual duties and methods used to deliver products and services.

ISO IEC 27001:2013 is a generic ISM standard designed for use by any organization. It entails minimum internal prerequisites for evaluating and treating information security risks customized

[211] International Organization for Standardization. ISO/IEC 27001 International Standard..
[212] William M. Lankford, "ISO 9000: Understanding the Basics," *Review of Business*. Vol. 21, Issue No. 1 (2000)

to the specific organizational needs.[213] The purpose of the standard is to assist organizations in establishing and maintaining an ISMS. The standard comprises of ten fundamental clauses.[214] Clause 1 deals with the scope and this has to do with general requirements for an ISMS which can be deployed in an organizational entity of any size or type. Clause 2 is concerned with normative references. This refers to an overview and vocabulary, which is referenced and offers valuable guidance. Under clause 3 we have terms and conditions where the standard references ISO/IEC 27000 for all terms and definitions. Clause 4 deals with organization context. The standard requires organizations to evaluate and account for all external and internal factors that could deter successful implementation of ISMS.[215] Such factors may include environmental conditions, contractual and legal obligations, formal governance policies, organizational culture and regulatory requirements. The clause also requires an organization to decide on the scope of ISMS, which needs to relate with the overall strategic direction, core objectives and expectations of interested parties. Organizations are further expected to show how they will go about establishing, implementing, sustaining and continually improving the ISMS in regard to the standard.

Clause 5 is the leadership clause. This clause requires senior managers within corporate entities organizations to formulate information security policies, to offer overall leadership by assigning responsibility and authority to implement the policies and to actively promote an organization-wide understanding of the significance of information security. Clause 6 is on planning and it calls for assessment of organizations' specific risks regarding information security and

213 International Organization for Standardization *Information Security Management Systems Requirements*. https://www.iso.org/standard/54534.html (Accessed on March 20, 2018)

214 The BSI Group. ISO/IEC 27001:2013 Implementation Guide. https://www.bsigroup.com/LocalFiles/en-GB/iso-iec-27001/resources/ISO-27001-implementation-guide.pdf (Accessed on March 23, 2018)

215 Ibid.

formulating treatment plan to tackle the risks. This clause provides reference for possible risk management mechanisms, but organizations are eventually responsible for determining specific control measures necessary to address identified risks.[216] The clause thus points out the need to introduce information security objectives and the properties that information security objectives must have.

Clause 7 and 8 are on support and operation respectively. Under support, the standard requires organizations to avail necessary resources towards the establishment, implementation, maintenance and continuous improvement of ISMS. This clause also requires all personnel working under an organization's control to be conversant with the information security policy, their contribution to its effectiveness and consequences of not conforming.[217] It further requires control of accessibility to documented information about the ISMS. The operation clause documents execution of policies, processes and practices and requirements for maintenance of appropriate records that reflect the outcomes. It also specifies the conduct of performance evaluation at scheduled intervals and implementation of the risk treatment plan. Clause 9 is concerned with Performance Evaluation and it requires organizations to monitor, measure, analyze and evaluate ISMS at prearranged timing to assess its efficacy and suitability. Clause 10 is the final clause of the standard and it embraces the principle of continuous improvement and the need for identification of nonconformities and taking corrective measures to enhance the efficacy of the ISMS. Non-conformities must, in this regard, be evaluated, corrected, and

[216] The BSI Group. ISO/IEC 27001:2013 Implementation Guide. https://www.bsigroup.com/LocalFiles/en-GB/iso-iec-27001/resources/ISO-27001-implementation-guide.pdf (Accessed on March 23, 2018).
[217] Ibid.

documented, so as to prevent their recurrence.[218] The provisions under the ten clauses are summarized in Table 1 below.

Table 1: Summary of ISO/IEC 27001:2013 Clauses

Clause Number	Item	Clause Description
Clause 0	Introduction	Introductory clause
Clause 1	Scope	General Requirements
Clause 2	Normative References	Overview and vocabulary which is referenced for appropriate guidance.
Clause 3	Terms and definitions	Definition of Terms and Concepts
Clause 4	Context of the organization	Internal and external organizational analysis in terms of the ISMS standard.
Clause 5	Leadership	Formulation of information security policy and promotion of organization-wide understanding of the significance of information security.
Clause 6	Planning	Assessment of institutional information security risks and developing appropriate mitigation measures.
Clause 7	Support	Provision of necessary resources, generation of awareness on information security policy and control of access to documented information about the ISMS.
Clause 8	Operation	Execution of the policies, processes and practices covered in the earlier clauses
Clause 9	Performance Evaluation	Monitoring, measuring, analyzing and evaluation of ISMS at prearranged intervals to assess its suitability and effectiveness.
Clause 10	Improvement	Identification of nonconformities, corrective action and continuous improvement

SOURCE: *BSI. ISO/IEC 27001:2013 Implementation Guide*

Besides the above clauses, ISO/IEC 27001:2013 also encompasses Annex A, titled "Reference Control Objectives and Controls." Controls in this case refers to avenues to risk management, for instance, institutional designs, regulations, protocols, conditions and practices, whilst control objectives are basically statements describing desired ends resulting from implementing

[218] Lois Evans, "Protecting Information Assets Using ISO/IEC Security Standards," *Information Management*, November-December 2016

controls.[219] This annex identifies 114 specific controls and 35 control objectives on Information security management. These controls are categorized under 14 different "Information security control code of practice," [220] as follows:

Table 2: Reference Control Objectives and Controls

Annex No.	Item	Description
A.5:	Information security policies (2 controls)	Covers how information security policies are written, reviewed and revised.
A.6:	Organization of information security (7 controls)	Details how responsibilities are assigned. It also encompasses controls for mobile equipment and teleworking.
A.7:	Human resource security (6 controls)	Addresses controls prior to, during and after employment.
A.8:	Asset management (10 controls)	Encompasses hard and soft assets, including information categorization and media handling.
A.9:	Access control (14 controls)	Covers all aspects of access, for instance, accessibility control requirements, user accessibility controls and application and system management and access.
A.10:	Cryptography (2 controls)	Addresses encryption and fundamental management controls.
A.11:	Physical and environmental security (15 controls)	Details controls applicable to secure areas and equipment.
A.12:	Operations security (14 controls)	Includes controls applied to IT security operations, for instance, operational software control, protection from malware, logging and monitoring, backup, technical vulnerabilities management and audit considerations.
A.13:	Communication security (7 controls)	Encompasses controls associated with network security, network services, segregation, information exchange and messaging.
A.14:	System acquisition, development and maintenance (13 controls)	Addresses controls for information systems security requirements and security in development and support processes
A.15:	Supplier relationships (5 controls)	Covers controls for monitoring suppliers throughout the supply chain.

[219] Lois Evans, "Protecting Information Assets Using ISO/IEC Security Standards," *Information Management*, November-December, 2016

[220] Alexander Haubler. *ISO 27001: Information Security and the Road to Certification*. TUV SUD America, 2015, 5

Annex No.	Item	Description
A.16:	Information security incident management (7 controls)	Includes controls for reporting security events and vulnerabilities, response protocols and the collection of evidence.
A.17:	Information security aspects of business continuity management (4 controls)	Details controls needed for purposes of secure business continuity, including procedures, verification practices and system redundancy.
A.18:	Compliance (8 controls)	Applies to the controls needed to identify applicable security legislation and regulations and the conduct of information security reviews

SOURCE: *BSI. ISO/IEC 27001:2013 Implementation Guide*

The above reference objectives and control items are offered as possible risk control processes for addressing the requirements spelt out in Clause 6 of the standard. Nonetheless, organizations make independent determination of appropriate control mechanisms needed to address specific risks faced.[221]

2.8.4 Steps to Certification

ISO certification implies that organizational systems meet established quality standards.[222] Implementing ISMS as per the requirements of ISO/IEC 27001 and obtaining certification entails a number of steps. Nevertheless, not all ISMS implementation efforts are similar, since individual organizations have unique issues to address and also differ in terms of system readiness.[223]

Successful execution of any managerial system, ISMS included, calls for first and foremost, commitment of the top leaders of an organization. Without such commitment, the other areas of

[221] Alexander Haubler. *ISO 27001: Information Security and the Road to Certification*. TUV SUD America, 2015, 5
[222] Peter C. Brewer and Tina Y. Mills, "ISO 9000 Standards: An Emerging CPA Service Area," *Journal of Accountancy* 177, No. 2 (1994)
[223] Haubler. op.cit, 6

emphasis will ultimately hinder the implementation effort. The organization will thereafter identify and define information security policies centered on the particular goals it strives to attain. These policies serve as a blueprint for future advancement efforts by way of spelling out the strategic direction and an array of guidelines regarding information security. With the information security policy in position, an organization goes on to identify the exact areas of IT system security that can be successfully handled within the parameters of its ISMS, while making reference to specific guidelines as highlighted under scope above.

Employing the most suitable procedure, an organization thereafter carries out an extensive risk evaluation to highlight both system vulnerabilities as well as administrative threats that need to be addressed. Risk assessment also creates the basis as well as rationale for mitigation measures.[224] The organization accordingly deploys strategies and activities to tackle all risks established from the risk evaluation. The outcome of these strategies and undertakings are then analyzed and altered accordingly to enhance their effectiveness. With organizational risks examined and ascertained and appropriate frameworks instituted, the organization carries out a pre-audit certification evaluation exercise to determine possible concerns that could have a negative effect on certification audit results. Any non-compliance with standard provisions are then addressed and/or corrected.

Finally, an independent and duly authorized certification agency is employed to carry out formal audit in relation to adherence to ISO/IEC 27001 requirements. A positive audit outcome leads to endorsement for certification where the certificate is granted by the certification body. [225]

[224] Chunlin Liua et al. The Security Risk Assessment Methodology. International Symposium on Safety Science and Engineering in China, 2012, 601

[225] Alexander Haubler. *ISO 27001: Information Security and the Road to Certification*. TUV SUD America, 2015, 6

Organizations that attain ISO/IEC 27001 certification are subjected to annual surveillance audits to ascertain continued adherence to the requirements of the standard. Full re-certification audits are further required to be undertaken every third year after the certification/recertification date.

2.9 BENEFITS OF ISMS

Information together with the supporting systems, processes and networks are crucial business assets of an organization.[226] If an organization seeks to maintain a comparative advantage, favourable cash flow position, profit orientation, positive corporate image and legal compliance, then security of its information assets is of great significance. In the contemporary era, organizations are more and more faced with increasing number of threats which include sabotage, espionage, computer-assisted fraud and vandalism. Other threats facing organizations include malicious code, computer hackers and denial of service attacks. Therefore, adoption of protection measures to safeguard information systems and to bar unlawful accessibility, application, interference, disclosure, alteration, perusal, inspection, destruction or recording is vital.

The embracing of ISMS by an organization brings with it several advantages. These include existence of a structured way of managing information security within an organization and conformity to the best business process practices.[227] It also enhances information security governance leading to an increase in information security levels within the organization. This

[226] K.C. Laudon andJ.P. Laudon. *Management Information System*. (New Delhi: Pearson Education, 2016).

[227] Indian Register Quality System. *Information Security Management System*. http://www.irqs.co.in/information-security-management-system.html (Accessed on February 15, 2018)

ultimately contributes towards the elevation of an organization's global positioning and reputation.

On the part of commercial entities, top management can leverage ISMS certification in a bid to gain new business. Achieving certification puts an organization on the radar to gain business from sectors where information security is critical. It offers an assurance of the organization's commitment towards protection of information assets. Advertising certification to a universally accepted information security standard significantly increases chances of attracting potential customers and stakeholders. With higher product quality and certified quality systems, organizations thus possess a comparative advantage in satisfying consumer needs and ultimately acquiring new customers.[228]

ISMS certification through the ISO 27001 standard focuses primarily at the entirety of an institution's information assets and processes that estimate risks facing these assets. Participants in the process look at the likelihood of an attack or failure, the effect that such an attack or failure would have on the organization and the efficacy of controls intended to safeguard the assets. Certification thus increases reliability and security of the systems. More importantly, it helps in reducing risks against information assets, hence cost of breaches, besides also ensuring cost-effective and consistent information security.[229]

Certification of an entity's ISMS helps in ensuring that the institution has a structure for generating, deploying, operating, analyzing, enhancing and sustaining security of information

[228] Amir M. Hormozi, "Understanding and Implementing ISO 9000: A Manager's Guide," *SAM Advanced Management Journal* 60, no. 4 (1995)

[229] Indian Register Quality System. *Information Security Management System*. http://www.irqs.co.in/information-security-management-system.html (Accessed on February 15, 2018)

including customer information being held by the organization. The ISMS guarantees handling of overall business risks by implementing security controls tailored to the conditions of the organization thereby enhancing productivity and fostering positive corporate image.[230] Certification also demonstrates top management commitment to upholding security of information assets. It further helps to ensure contingency planning, improved risk management and integration of information security concerns with other management systems.

The ISO standard on ISMS specifies the conditions for administering and sustaining an effective ISMS to safeguard against the root sources of information security risks. Organizations that achieve ISO/IEC 27001 certification strengthen their ability to safeguard themselves against cyber-attacks and help avoid unauthorized access to sensitive or confidential information.[231] The use of ISO standards helps in creation of safe, reliable and good quality products and services. Standards help organizations increase productivity by reducing errors and waste. By directly comparing products from different markets, companies are able to venture into new markets and help develop global trade fairly. The rules also serve to protect consumers and end users of commodities and services, guaranteeing that certified products comply with internationally recognized minimum acceptable standards.[232]

ISO standards facilitate trade, disseminate knowledge, innovative technological advances and share progressive governance and evaluation methods. They offer remedies and realize merits for virtually all business sectors, including construction, agriculture, manufacturing, mechanical

[230] Indian Register Quality System. *Information Security Management System*. http://www.irqs.co.in/information-security-management-system.html (Accessed on February 15, 2018).
[231] Alexander Haubler. ISO 27001: *Information Security and the Road to Certification*. TUV SUD America, 2015, 3
[232] International Organization for Standardization. *All About ISO*. https://www.iso.org/about-us.html(Accessed on February 15, 2018)

engineering, transportation, distribution, environment, medical, ICT, and energy. ISO develops benchmarks for which there exists clear market requirement. The work is done by industry experts drawn from industrial, technical and commercial sectors that have identified need for the standard and who subsequently use the standard. These experts may be accompanied by others with relevant knowledge, for example, representatives of government agencies, test labs, consumer associations and academics, and international governmental and non-governmental organizations. An international ISO standard thus depicts global consensus regarding the subject of the standard.[233]

In the contemporary world economy, trade barriers have to a significant scale been eliminated. Corporate entities have in this regard raised their level of performance to survive the aggressive environment. To remain competitive, organizations must implement effective and efficient plans. The most accepted plan today is the ISO standard. [234] The standard provides guidelines that aid organizations to achieve quality assurance and cost effective methods of operation.

2.10 CHAPTER SUMMARY

This chapter has presented an analysis of the application of ICT in Africa and its impact on development. It has also outlined the risk factors emanating from the incorporation of IT and efforts made towards addressing information security concerns at the continental level. The chapter has further identified the overarching information security objectives in Africa and best practices in combatting information security challenges. Towards this end, the chapter

[233] International Organization for Standardization. *ISO Brief*. https://www.iso.org/files/live/sites/isoorg/files/archive/pdf/en/pub100288.pdf

[234] Anthony Nurre,Yusuf Gunaman and Dennis De-Almeida. *What It Means to be ISO 9000 Certified*. Research Paper. September 22, 2000.

highlighted three key approaches that could be pursued in securing African information assets with greater focus being paid on the ISO standard on information security. The next Chapter narrows down this analysis to the Kenyan context through examination of the institutional and policy structures established in the country towards addressing the broad-based security concerns.

CHAPTER THREE

KENYA'S INSTITUTIONAL AND POLICY FRAMEWORK ON INFORMATION SECURITY

3.1 INTRODUCTION

This chapter derives from the broader African information security management perspective as discussed under chapter two herein. The chapter focuses on the existing information security institutional arrangement in Kenya. It also provides highlights of the various laws and policies governing information technology. It further outlines key strategic action plans and existing linkages amongst different players in implementing information security programmes.

3.2 INSTITUTIONAL FRAMEWORK

Kenya's public sector ICT programmes are implemented through collaborative effort involving different stakeholders. These include Ministries, Departments and Agencies and also the general public. The overall coordination of the formulation, implementation and monitoring of these programmes and projects is vested with the Ministry of ICT, the Kenya ICT Authority of Kenya and the Communications Authority of Kenya. The specific area of contribution by each of the key players is elucidated below.

3.2.1 Ministry of Information, Communication and Technology

All ICT policy interventions in Kenya are centrally coordinated by the Ministry of Information, Communication and Technology. The Ministry was created together with its related entities with the responsibility to create and administer appropriate policy initiatives and development programmes geared towards producing ICT linked commodities and services needed by suppliers of these products and services in not only the government but also private agencies.[235]

The Ministry comprises of two State Departments, namely, the State Department for Broadcasting and Telecommunication and the State Department for ICT and Innovation. The responsibilities of the State Department for Broadcasting and Telecommunication include formulation of telecommunication and broadcasting policies, language policy management, coordination of public communications, national Government advertising, Government telecommunication and postal and courier services.[236] The responsibilities of the State Department for ICT and Innovation on the other hand entail formulation of national ICT policies, promotion of e-government, promotion of software development industry, provision of ICT technical support to MDAs, policy formulation on digitization of government services, developing national communication capacity and infrastructure and managing national fibre optic infrastructure.[237] For the effective discharge of its mandate, the Ministry has a number of State Corporations and Semi-Autonomous entities of the government. State Corporations encompass the Kenya ICT Authority, the Communications Authority of Kenya, Kenya

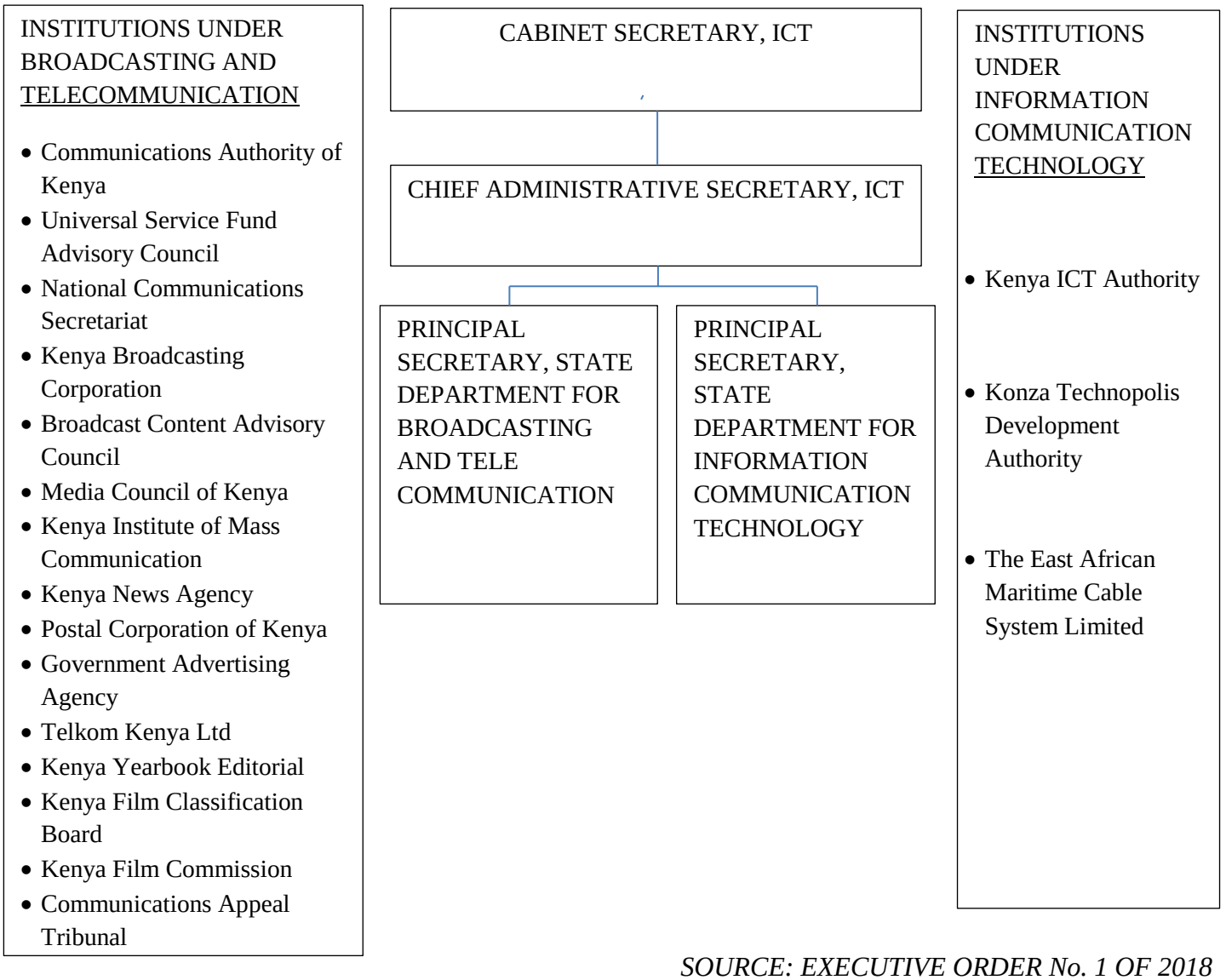
[235] Ministry of Information, Communication and Technology. *Strategic Plan, 2013-201.* (Nairobi: Ministry of ICT, 2013), 2

[236] Ministry of Information, Communication and Technology. *Functions of the State Department of Broadcasting and Telecommunicationt*. http://www.ict.go.ke/broadcasting-and-telecommunication/ (Accessed on June 20, 2018.

[237] The Presidency. Executive Order No. 1 of 2018. (Nairobi: Government Printer, 2018), 41

Broadcasting Corporation, Postal Corporation of Kenya, Konza Technopolis Development Authority and Media Council of Kenya.[238] Semi-Autonomous Government agencies include Kenya Institute of Mass Communication, National Communications Secretariat and Communications Appeal Tribunal.[239] The diagrammatic presentation of the Authority structure under the Ministry of ICT is given below.

Figure 3: Institutional Structure of the Ministry of ICT



SOURCE: EXECUTIVE ORDER No. 1 OF 2018

[238] The Presidency. Executive Order No. 1 of 2018. (Nairobi: Government Printer, 2018), 42

[239] Ministry of Information, Communication and Technology. *Functions of the State Department of Broadcasting and Telecommunicationt*. http://www.ict.go.ke/broadcasting-and-telecommunication/ (Accessed on May 10, 2018

3.2.2 Kenya ICT Authority

The Kenya Information and Communication Technology Authority is a State Corporation under the Ministry of ICT that was created vide Legal Notice No.183 of August, 2013. The Authority was created for purposes of establishing, developing and maintaining secure ICT infrastructure and systems for efficient and effective public services delivery as well as advancing the deployment and usage of ICT in Kenya. Its vision is "to be the leader in transforming Kenya into a regional ICT hub and a globally competitive digital economy". Its mission is "to champion and harness ICT for efficient and effective public service delivery, wealth creation and wellbeing of Kenyans."[240]

The Authority's key functions as defined under its Strategic Plan (2013-2018) include setting and enforcing ICT regulations and standards for infrastructure, human resources, protocols, technology and systems in public offices and the public service; deployment and management of public service ICT staff; facilitating and regulating the design of and spearheading use of ICT in the public sector; promoting ICT education and capacities; promoting digital government initiatives; facilitating optimal e-records, electronic forms and public sector equipment use; promoting IT enterprise and innovation; establishing, developing and maintaining secure ICT systems and infrastructure; overseeing the designing, development as well as implementation of vital ICT projects in the public sector and implementing and managing the Kenya National Spatial Data scheme.[241]

[240] Kenya ICT Authority. *Strategic Plan, 2013 – 2018*. (Nairobi: ICTA, 2013), 11.
[241] Ibid., 9.

3.2.3 Communications Authority of Kenya

The Communications Authority of Kenya is the regulatory authority for Kenya's communications sector. [242] Established in 1999 through the Kenya Information and Communications Act, 1998, the Authority is mandated with facilitating development of information and communications segments including broadcasting, telecommunications, electronic commerce, multimedia, postal and courier services.

The Act specifically mandated the Authority to come up with a national cyber security administration blue print via the formulation of national computer incidents response team. Towards this end, the Authority setup the Kenya Computer Incident Response Team (KE-CIRT) Coordination Center to facilitate effective administration of cyber security issues. The KE-CIRT is the country's trusted cyber safety combat point and the unit is tasked with playing an advisory role on issues concerning cyber security as well as coordinating appropriate response to identified cyber cases in liaison with specific stakeholders nationally, within the region and also on the global front. Its mandate area also includes gathering and dissemination of technical details pertaining to computer security cases; carrying out studies on computer security; data security capacity development, awareness creation on cyber security-related undertakings; and, fostering the establishment of National Public Key Infrastructure.[243]

[242] Communications Authority of Kenya. *Strategic Plan 2013 – 2018*. (Nairobi: Communication Authority, 2013), 1
[243] Communications Authority of Kenya. *About Us*. http://www.ke-cirt.go.ke/index.php/about-us (Accessed on 23rd March, 2018)

3.2.4 Ministries Departments and Agencies

The various MDAs are responsible for implementation of ICT programmes within their respective areas of jurisdiction. This includes planning, budgeting and monitoring implementation of individual programmes and projects concerning a particular line Ministry and/or Department. The MDAs are also individually accountable for budgetary allocations made against their respective votes towards ICT under both recurrent and development levels of expenditure. Periodic reports are thereafter prepared by the MDAs highlighting strides made in implementing ICT programmes and projects. These reports are shared with relevant agencies including Ministry of Information, Communication and Technology, Kenya ICT Authority and also the performance contracting division under the Executive Office of the President to the extent that performance contract commitments are concerned.

3.3 LEGAL AND POLICY FRAMEWORK

The Government has commissioned a number of policies relating to information management. These policies have been anchored on various legal instruments, among them being the Constitution of Kenya, 2010, the Kenya Information and Communication Act, 2015, the Access to Information Act, 2016, the Critical Infrastructure Bill, 2015 and the Computer Misuse and Cyber Crimes Act, 2018.

Kenya Vision 2030 is a long term national development road map that targets transforming the country into a middle income, globally competitive state, offering top notch quality of life for every citizen by 2030. ICT has been highlighted as a strategic driver towards actualizing the

Vision and the long-term strategic perspective for ICT is in this regard well-articulated therein. The business process outsourcing sub-sector alone is projected to generate in excess of twenty thousand job opportunities and generate over 10 per cent to country's gross domestic product during the plan period. The projections comprise of development of a robust IT sector so as to spur growth as well as propelling production capacity and progress in other growth spheres, encompassing tourism, agriculture, manufacturing, entertainment and financial sectors.[244] ICT is also projected to impact on and foster accountability, equity, as well as transparency in the socio-political domains, required for creation of wealth and job opportunities. Further, ICT is identified as being critical in promoting good governance as well as operational efficiency across all sectors of the economy resulting in improved delivery of public services.

Arising from propositions under Vision 2030 and subsequent constitutional provisions, the Ministry of Information, Communication and Technology formulated a 5-year strategic plan in 2013 which continues to guide its operations. The plan focuses on reaffirming the basis of a competitive knowledge-oriented society through legal, policy, institutional and regulatory reforms, country-wide network broadband connectivity, digital government and economy, enhancement of ICT capability, strong private-public partnerships, applications and content development, creation of wealth and jobs as well as mainstreaming of crosscutting matters.[245]

The Kenya ICT Authority also operates under a five year strategic plan that covers 2013 to 2018 period. Among other considerations, the Strategic Plan is aimed at deepening and strengthening the automation foundation so as to transform Kenya into a knowledge-based and globally

[244] Republic of Kenya. *Kenya Vision 2030*. (Nairobi: Government Printer, 2007), 14
[245] Ministry of Information, Communications and Technology. *Ministerial Strategic Plan*. (Nairobi: Ministry of ICT, 2013), viii.

competitive nation. This transformation is to be done by fostering and inspiring ICT investment by expanding ICT connectivity and providing less costly services that can be accessed by all.[246]

The Government also launched the national ICT Master Plan in February 2013 with a view to, among others, extending involvement of stakeholders as well as putting into perspective new developments regarding implementation of a digital Government. The Master Plan was arrived at following various consultation engagements with stakeholders, both public and private agencies' document reviews, analysis of other countries' Master Plans as well as comparing and benchmarking the different growth indices against other advanced and emerging economies. The Master Plan also seeks to align the ICT sector with key documents, for instance the constitution, and in particular, realities of devolved system of Government and new legislations adopted between late 2012 and early, 2013 including the Science, Technology and Innovation Act 2013, Universities Act 2012 and TIVET Act 2013. This is because ICT plays a fundamental role in guiding Kenya's socio-economic and political development, as advocated in Vision 2030 and that it is an avenue towards knowledge based society that will in turn spur socio-economic growth. The Master Plan underlines the need to tackle key hindrances that may affect the ICT industry from discharging its contribution to national development.[247] It thus falls within the purview of the Vision 2030 and its attendant Medium Term Plans and is generally aimed at placing the country at an apex position of an ICT hub and also attain a digital competitive edge in the global economy.

As Kenya matures into an information society, it continues to encounter an ever-changing landscape of cyber threats. States, criminal organizations and hacktivists are and will continue to

[246] Kenya ICT Authority. *Strategic Plan, 2013 – 2018*. (Nairobi: ICTA, 2013), 25.
[247] Kenya ICT Authority. *Kenya National ICT Master Plan*. (Nairobi: ICTA, 2013), 13.

exploit ICT vulnerabilities.[248] This is a reality faced by all countries with strong ICT resource base. Whilst these actors strive to illegally access, interfere, destroy or distort sensitive government, commercial and personal data, the country has been working diligently towards development of information protection channels so as to respond to both current and prospective risks on the horizon. Recognizing the realities of cyber threats and understanding the fundamental role of ICT on the Kenyan economy, the Government has further developed the national cyber security strategy. This strategy feed into the three pillars of Vision 2030 and other national programmes including the ICT master plan. It outlines the country's cyber security vision, principal aims and ongoing efforts to facilitate national priorities by promoting expansion of ICT and vehemently safeguarding critical IT information infrastructure.[249] It also demonstrates the commitment of the state to the security and prosperity of the nation. Successful implementation of the strategy is expected to enable Kenya attain societal and economic objectives via a safe online space for industry, citizens and foreign ent6ities to carry out business[250]. Noting that cyber security is a shared responsibility, strategy implementation envisages a collaborative effort between the government, academia, private sector and other non-governmental entities.

The realization of an information society and knowledge based economy is a priority item for the Government of Kenyan in its pursuit of development outcomes and objectives for employment and wealth creation.[251] Towards this end, the Government reviewed the ICT policy of March 2006 and developed National ICT Policy 2016. The policy review was driven by the need to revise ICT policies so as to conform to the country's 2010 Constitutional order and the Vision

[248] Ministry of Information, Communication and Technology. *National Cyber Security Strategy*. (Nairobi, 2013), 5
[249] Ibid.
[250] Ibid., 1
[251] Ministry of Information and Communication. *National Information Communication and Technology Policy*. (Nairobi: MICT, 2016), 2.

2030. The revision also intended to offer proactive regulatory and policy framework that adheres to present-day conditions and changes in technology and also steer systematic ICT sector advancement in order to enable maximum impact for the benefit of every Kenyan. In the formulation of the new policy, the Government took into consideration the tremendous effect of globalization as well as frequent technological changes. These transformations have significantly shaped the traditional methods of managing public affairs and the provision of services, which essentially informs the need for a more pro-active regulatory, procedural and policy reaction. The main objective entails provision of access to ICT, in particular broadband for all Kenyans and a smooth connection with member states of the East African Community while instituting proactive partnership not only at the regional level, but also on a global scale. The policy generally seeks to set the pace for further ICT industry advancement and the economic progress whilst guaranteeing that every stakeholder gains from the eventual benefits. It provides a roadmap to guide economic, political, cultural and social transformation through effective usage of IT in the years ahead.[252]

3.4 CHAPTER SUMMARY

From the above analysis, it is clear that the Kenyan Government has established an elaborate institutional and policy framework towards implementation of ICT programmes. It is also clear that matters regarding information security have been accorded due consideration in the design of the policy instruments. Further, it is evident that the Government has produced various strategic documents geared towards guiding the roll-out of government policies on ICT amongst the MDAs and other levels. The extent to which the ISMS has been incorporated amongst these policies and strategies, existing gaps, if any, and future prospects is examined in the next chapter.

[252] Ministry of Information and Communication. *National Information Communication and Technology Policy*. (Nairobi: MICT, 2016), 2.

CHAPTER FOUR

EXTENT AND EFFECT OF APPLICATION OF ISMS PRINCIPLES IN KENYA'S PUBLIC SECTOR POLICY ENVIRONMENT

4.1 INTRODUCTION

This chapter goes beyond the mention of institutional, legal and policy instruments, as highlighted under chapter three, by looking at the status of incorporation of information security and ISMS in the legislative and policy tools. In particular the chapter examines the level to which the guiding principles of ISMS have been entrenched in the country's policy framework and institutional arrangement. It also draws a nexus between ISMS and national development with specific focus on setups of the various MDAs. The study findings and observations made herein are based on key informant interviews, administration of observation check-list and other related data sources.

4.2 STATUS OF IMPLEMENTATION OF INFORMATION SECURITY STANDARDS

Information security concerns have been addressed variously in a number of legal and policy instruments. These include laws, policies and guidelines, as discussed below.

4.2.1 Implementation of Principles of Information Security Through Legislation

Legislative instruments containing aspects of information security include the Computer Misuse and Cyber Crimes Act, the Kenya Information and Communication Act, the Access to Information Act and the Critical Infrastructure Bill, 2015. An analysis of relevant provisions under each of the above legal instruments is provided below.

(a) Computer Misuse and Cyber Crimes Act, 2018

The Computer Misuse and Cyber Crimes Act, provides for the establishment of a countrywide coordination committee on computer and cybercrime issues. The committee comprises, among others, the Principal Secretary tasked with matters pertaining to internal security, the Principal Secretary responsible for information and technology, the Chief of the Military Forces of Kenya, the Director General of the National Security Intelligence Service, National Police Service Inspector General and the Attorney General. [253] The functions of the committee shall be to advise the Government on security issues associated with chain technology, vital infrastructure, e-commerce and trust accounts; advise the Kenya National Security Council on computer and cybercrimes; co-ordinate national security organs on matters concerning computer and cybercrimes; receive and act on reports regarding computer and cybercrimes; create a mechanism to enable availability, integrity as well as privacy of important data resources of the nation encompassing national telecommunication and data systems; co-ordinate gathering and evaluating data on cyber risks as well as response to cyber cases that endanger the country's cyberspace, whether such threats or computer and cybercrime incidents occur within or outside

[253] Republic of Kenya. Computer Misuse and Cyber Crimes Act, 2018. (Nairobi: Government Printer, 2018), 47.

Kenya; co-operate with computer incident response team and other relevant entities locally and internationally on response to threats of cybercrime and incidents; establish cyber-security practice codes and performance standards for implementation by owners of critical information infrastructure; develop and manage national public key infrastructure and develop a mechanism for training on prevention and mitigating computer and cybercrimes and matters associated thereto.[254] The Act further provides for the formation of a secretariat to the committee comprising of the Director and such number of public officers that, subject to approval of the Committee, the Cabinet Secretary tasked with matters pertaining to internal security in liaison with the Cabinet Secretary mandated with matters regarding information, communications and technology may deploy to the Secretariat.

Section 14 (1) of the Act stipulates that an individual that instigates, either permanently or temporarily, a computer system to execute tasks, through breaching security protocols purposely to gain access, and is aware that this accessibility is not authorized, commits a transgression and is culpable to a fine that amounts to five million shillings or up to three years' jail term, or both.[255] Section 16 (1) provides that an individual who with intent and no authorization performs any undertaking that produces interruption to computer systems, applications or information, makes a crime and is culpable to a fine to the tune of ten million shillings or up to five years' prison term, or both.[256] For clarity reasons, the section interprets an interruption as unauthorized in instances where individuals whose actions result in the interruption are not mandated to cause the interruption nor have the permission to cause the interruption from entitled individuals..

[254] Republic of Kenya. Computer Misuse and Cyber Crimes Act, 2018. (Nairobi: Government Printer, 2018), 48.
[255] Ibid., 52
[256] Ibid., 53

Section 17 (1) further states that an individual who with intent and no authorization performs any undertaking that diverts or results in interception, either directly or indirectly and initiates transmission of data against computer connections via telecommunication systems performs a transgression and is culpable to a fine amounting to ten million shillings or up to five years' imprisonment, or both. [257] Under Section 18 (1), an individual who intentionally develops, inherits, imports, purchases for use, offers to supply, distributes or through any other means makes available devices, programs, access codes, passwords, or equivalent aids tailored or adjusted mainly with the aim of executing a violation of the provisions of the Act, does an offence and is culpable to a fine amounting to twenty million shillings or up to ten years' imprisonment or both. [258]

Section 19 (1) states that an individual who with intent and illegally discloses any password, accessibility code or other ways of gaining access to any programme or data held in any computer system commits an offence and is culpable to a fine amounting to five million shillings or up to three years' prison term, or both. [259] A person who commits the above offence for any unlawful gain, any wrongful purpose or to bring about any loss, is culpable to a fine amounting to ten million shillings or up to five years' prison term, or both.

Under Section 21 (1), an individual who illegally and with intent performs or authorizes or allows another individual to perform a prohibited act as enshrined in the Act, so as to gain access to critical data, critical database or national critical information infrastructure or intercept data, to from a critical database or a national critical information infrastructure with the intent of

[257] Republic of Kenya. Computer Misuse and Cyber Crimes Act, 2018. (Nairobi: Government Printer, 2018), 54
[258] Ibid., 55
[259] Ibid., 56

directly or indirectly benefitting foreign countries against the Republic of Kenya, commits an offence and is liable to a fine amounting to ten million shillings or a prison term extending to twenty years or both. [260] The section further provides that an individual who unlawfully and knowingly performs or authorizes, or allows another individual to perform a prohibited act as envisaged under the Act in a bid to gain access to, or intercept data, which is in possession of the State and which is exempt information according to the law relating to access to information, with the intention of directly or indirectly benefitting foreign nations against the Republic of Kenya, commits an offence and is liable, on conviction , to a fine amounting to five million shillings or up to ten years' prison term, or both.[261] Finally, Section 8 of the Act requires the Committee to submit reports on matters regarding misuse of computers and abuse of cyber space to the National Security Council at the end of every quarter. [262]

(b) Critical Infrastructure Bill, 2015

The Critical Infrastructure Bill, 2015 provides for the formation of Critical Infrastructure Protection Unit to coordinate and reinforce issues regarding protection of important infrastructure in the country.[263] In a bid to stem rising cases of interference with vital installations including power lines, optical fibre cables, information centers and road infrastructure, the bill stipulates heavy fines and jail terms of up to ten years for individuals found culpable of sabotaging infrastructure that is essential to the country's security interests. It accentuates the need for a holistic strategy in planning, structuring and installation of vital infrastructure

[260] Republic of Kenya. Computer Misuse and Cyber Crimes Act, 2018. (Nairobi: Government Printer, 2018), 57
[261] Ibid., 58
[262] Ibid., 48
[263] Paul Kinuthia. *Critical Infrastructure Bill, 2015*. https://www.scribd.com/document/324737125/Critical-Infrastruture-Bill-2015-Review (Accessed on March 20, 2018).

resources such that ICT sub-elements are incorporated.[264] The Critical Infrastructure Protection Unit, is empowered to obtain from any party any information on CCTV, building plans, drawings and other related items for incorporation in information registers. It identifies optical fiber cables, telecom lines, submarine cables and posts as vital ICT resources. The national security camera database, routers, hosting batteries, power units, Kenya Power meters, as well as cutouts and high definition cameras are other critical infrastructure identified by the bill.[265] Identified threats include espionage, sabotage, terror attacks, cyber-crimes, transgressions aimed at vital information infrastructure as well as vandalism. The unit is expected to work closely with the Inspector General, National Police Service, in ensuring that important infrastructure resources are accorded constant surveillance and secured from potential risks including interference through malicious use of force, terrorism other related undertakings.[266] The unit is also expected to consolidate information from the various owners of critical infrastructure resources so as to register, record its location and create a country-wide database of essential infrastructure.

(c) Kenya Information and Communication Act, 1998 (Revised 2015)

The Kenya Information and Communication Act provides for, inter alia, the creation of Communications Authority, to foster ICT sector development, including growth in broadcasting, multimedia, telecommunications and postal services and electronic commerce for connected purposes.[267] The Authority's functions with regard to electronic transactions include facilitating

[264] Paul Wafula. *Kenya To Set Up Unit to Protect Critical Infrastructure*. Standard Newspaper, Wednesday, 2nd September, 2015.
[265] Ibid.
[266] Ibid.
[267] Republic of Kenya. *Kenya Information and Communication Act*. (Nairobi: Government Printer, 2015), 9.

the e-transactions as well as cyber security. This is to be attained through, inter alia, utilization of credible e-records; enabling e-commerce and removal of obstacles to e-transactions, for instance, those arising from signature uncertainties and writing conditions; promotion of public trust in the reliability and integrity of e-records as well as e-transactions and the attendant cyber security issues; fostering development of e-commerce by employing electronic signatures to aid in the authentication process and guarantee integrity of correspondence on e-platforms; promoting and facilitating of efficient service delivery by public sector entities through reliable electronic records; developing sound frameworks to reduce cases of forging of e-records and electronic commerce fraud amongst other e-transaction and cyber space related concerns; promoting and facilitating of effective critical internet infrastructure management as well as developing an elaborate framework for investigating and prosecuting cyber based crimes.[268] The Authority is through the National Kenya Computer Incident Response Team facilitating coordinated response and effective management of cyber security incidents to ensure full implementation of the Act.

(d) Access to Information Act, 2016

Pursuant to Article 24 of the Kenyan Constitution, Article 6 (1) of this Act provides that the right of access to information shall be restricted in relation to material whose dissemination could compromise the security of the nation; interfere with due law processes; jeopardize individual health, safety or lives; involve unnecessary intrusion into the privacy of individuals, other than applicants or persons on whose behalf applications have, with express authority, been lodged; significantly dent commercial interests, encompassing institutional or third party intellectual property rights; cause significant harm to Government's ability to manage the economy;

[268] Republic of Kenya. *Kenya Information and Communication Act*. (Nairobi: Government Printer, 2015), 55.

immensely undermine private or public entities' capacity to offer sufficient and careful reflection of issues where no final decisions have been made and therefore remain subjects of active focus; cause harm to public entities' position on contemplated or actual legal processes; or violate professional privacy as documented in law or recognized by the rules of a duly registered professional body. [269]

Further to the above provisions, Article 6 (2) stipulates that information regarding national security consists of military plans, covert strategies, doctrines, capabilities, deployment and capacity; foreign state data with repercussions on domestic security; intelligence undertakings, capabilities, sources, cryptology or procedures; international relations; technological, economic or scientific issues associated with the nation's security; capabilities or susceptibilities of existing systems, infrastructure, installations, plans, safety services or ventures regarding the country's security; data prepared or obtained by state entities, and in particular, an investigative authority in the process of conducting legitimate inquiries pertaining to detecting, suppressing or preventing crime, implementing any legislation and actions suspected of translating to threats to the overall security of the nation; data between county and national governments considered to be detrimental to the operations of both categories of government within the authority structure; cabinet discussions and minutes; information that ought to be submitted to a constitutional commission, state organ or an independent office when carrying out tests, examinations, investigations, evaluations or audits in the discharge of its mandate; information identified as classified under the Kenya Defence Forces Act; and any other type of information whose divulgence would compromise state security.

[269] Republic of Kenya. *Access To Information Act No. 31 of 2016*. (Nairobi: Government Printer, 2016), 5.

A public agency is not under obligation to provide a requester with information if the information can be fairly accessed by alternative means. In determining public interest, the Act states that specific attention shall be paid to the provisions of the constitution on the need to enhance government entities' accountability to the public; ensure that use of public funds is subjected to an oversight process; foster debates on matters of mutual interest and public concern; have the public sufficiently informed of any potential risk against public health or safety or to the ecosystem and make certain that statutory bodies with regulatory mandates undertake their duties adequately.[270]

Article 7 of the Act provides for assignment of information access officer by public entities. Where a member of public desires to access information from a public entity, the Act provides that he/she will be required to formally file an application with the information access officer in in either English or Kiswahili and the applicant is expected to avail sufficient details to enable the information access officer or other relevant official to clearly figure out the information being sought. Soon after the data access officer has determined whether or not to grant access to information, immediate communication of the decision is supposed to be made to the requester. This communication should specifically indicate whether the public agency is in possession of the information being sought and/or whether an approval has been granted to access the information.[271]. In the event accessibility is denied, the reasons behind the decision is also communicated to the applicant.

Section 17 of the Act provides for management of records. Towards this end, the Act stipulates that all public agencies shall store and sustain reliable, useable and factual records in a way that

[270] Republic of Kenya. *Access To Information Act No. 31 of 2016*. (Nairobi: Government Printer, 2016), 5.
[271] Ibid., 6

will simplify accessibility to information. At the minimum, every public entity is required to establish and maintain information pertaining to decisions, transactions, policies, guidelines and specific activities undertaken in the execution of the institutional mandate; certify that information under its jurisdiction, inclusive of those stored electronically, are kept in an organized and decent state; and that within three year period from the date of commencement of the Act computerize individual data management systems and records so as to enable more efficient information access.[272]

4.2.2 Implementation of Principles of Information Security Through Strategy and Policy Documents

The study identified five major policy instruments where matters concerning information security have been incorporated. These are the Ministry of ICT Strategic Plan, the Kenya ICT Authority Strategic Plan, the Kenya ICT Master Plan, the National Cyber Security Strategy and the draft National ICT Policy. A detailed analysis of these policy instruments is provided below.

(a) Ministry of ICT Strategic Plan (2013 – 2017)

The Ministry of ICT strategic plan is anchored on eight broad areas of strategic focus. These are institutional, regulatory, policy and legal reforms; broadband network connectivity with a countrywide scope, electronic government and economy; enhancement of ICT capacity; robust public-private partnerships including integration across the region and among counties; development of appropriate applications and content; creation of wealth and jobs and

[272] Republic of Kenya. *Access To Information Act No. 31 of 2016*. (Government Printer. Nairobi. 2016), 10

institutionalizing a range of crosscutting themes. The Strategy identifies cyber-crime, moral degradation owing to presence of undesirable internet content and application of ICT to undertake terrorism linked actions as some of the major threats facing the Kenyan ICT sector.[273] Key managerial issues that the Strategy sought to address include insufficient organizational, legislative, regulatory and policy transformations, deplorable IT infrastructure on a national scale, sub-standard service delivery systems within the public sector, limited ICT capacity and uncoordinated public information and communication.[274] Towards this end, the Strategy prioritized a number of programmes and projects. These include development and review of legal, policy, institutional and regulatory structures to foster advancement and ICT growth, development of new ICT resources, enhanced service delivery via electronic government service platform, building of capacity in the IT industry and collection, collation and dissemination of credible information so as to promote a knowledge-based society.[275]

The specific legal, institutional and policy reforms highlighted in the plan include finalization and operationalization of national cyber security framework, passing of information protection law and policy, passing of Information Access law and policy and finalization of infrastructure sharing policy.[276] The Plan also spells out strategies to be implemented to achieve universal broadband connectivity. Strategies bordering on information sharing and information security include creation of a broader network mechanism as well as network coordination centres to guarantee that individual county head offices employ broadband network modules with at least 4mbps capabilities for every entity, introduction of 4G network protocols to offer improved

[273] Ministry of Information, Communication and Technology. *Strategic Plan, 2013-2018.* (Nairobi: Ministry of ICT, 2013), 11
[274] Ibid., 19
[275] Ibid.
[276] Ibid., 20

bandwidth capabilities, establishing information centres intended to guarantee that public information of strategic value is deposited in safe spaces with low level risks and affordably delivered, enhancing cyber security so as to minimize risks of cyber-attack, develop improved and more secure networks from the hierarchy of the big national public channels to users and implementing Public Key Infrastructure to authenticate and authorize information and data systems throughout the country.[277] Further, the Strategy stresses the need to build capacity for computer incidence response for purposes of effective coordination of computer related incidences in the country. [278]

The Ministry of ICT in collaboration with the various stakeholders has progressively implemented the various strategies outlined in the Plan and a significant number of targets have since been met. The Ministry is in this regard working towards formulating a new Strategic Plan for the period 2018-2022 to be based on Medium Term III strategic framework of the Vision 2030.

(b) Kenya ICT Authority Strategic Plan (2013 – 2018)

The Kenya ICT Authority Strategic Plan identifies a number of threats to information assets and infrastructure. Key threats associated with technological developments include increased cyber insecurity in ICT systems associated with cloud computing, lack of an appropriate legislation to deal with emerging technologies and concepts and procurement challenges linked with massive

[277] Ministry of Information, Communication and Technology. *Strategic Plan, 2013-2018.* (Nairobi: Ministry of ICT, 2013), 21
[278] Ibid.

scaling of outsourced services.[279] Other threats include under-prioritization of the ICT sector in the allocation of resources and high competition for exchequer funding, uncoordinated projects that do not exploit synergies in the national government digital agenda and county government support for ICT, threat of parallel ICT structures in Government and inadequate awareness of the role of ICT in senior positions in all arms of national and county governments.[280]

The Strategy brings out five broad areas of strategic focus, namely, shared services through ICT infrastructure and information infrastructure; ICT innovations and enterprises; information security; enhancement of human capital and ICT Governance. [281] The information security component entails development and incorporation of information security standards and guidelines, implementation of the country's cyber safety strategy and master plan, strengthening the data security role of the ICTA, development of a risk evaluation action plan and undertaking periodic risk assessment of state data infrastructure. It also entails enhancement of information security capacity, implementation of public key infrastructure, ICT infrastructure appraisal and development and maintenance of a wide-ranging ICT asset register including document handling and classification methodology.

The Strategy emphasizes the need for strengthening the structure for more effective coordination across MDAs, enacting an improved legislation on cyber security, developing elaborate security benchmarks as well as developing adequate capacities and skills in the sphere of data security. It also underlines the need to develop the network structure and infrastructure layout and governance, eliminate unauthorized and ungenuine software, develop suitable network resource

[279] Kenya ICT Authority. *Kenya National ICT Master Plan*. (Nairobi: ICTA, 2013), 14.
[280] Kenya ICT Authority. *Strategic Plan, 2013 – 2018*. (Nairobi: ICTA, 2013), 15.
[281] Ibid., 23.

support skills as well as avail sufficient financial provision for continuity of operations. The envisaged outcomes out of the information security strategic objective and attendant strategies include effective masterminding of data security undertakings across the government and increased integrity, privacy, accountability and availability of state services.[282]

(c) Kenya ICT Master Plan (2013/14 – 2017/2018)

The ICT Master Plan has six driving principles, namely, non-segregation, equity and partnership; unbiased technology; good governance; safeguarding and preservation of the environment and offering incentives.[283] The Master Plan consists of three overarching foundations and pillars apiece. Foundations here refers to the basic conditions that must happen to lay the base of Kenya's transition to a knowledge-oriented civilization and position the nation an ICT hub in the region, whilst pillars are geared towards facilitating attainment of economic and social expansion and Vision 2030 targets. The first foundation of the master plan is that of investing in human capital and equipping the workforce on IT, whose aim is to develop quality ICT human resources as a prerequisite for a vibrant IT sector. Central to this is ascertaining that the advancement, deployment and utilization of ICTs are sustainable and constituent part of growth. The second foundation is that of connected ICT infrastructure that aims at providing the supporting network of assimilated infrastructures necessary to allow economically efficient supply of IT services and products to the population. The third foundation is the cohesive information infrastructure that targets to enhance electronic government services provision quality and facilitate the nation in transitioning into a knowledge-oriented community. This is by way of making certain that there

[282] Kenya ICT Authority. *Strategic Plan, 2013 – 2018*. (Nairobi: ICTA, 2013), 25.
[283] Kenya ICT Authority. *Kenya National ICT Master Plan*. (Nairobi: ICTA, 2013), 13.

exists optimum accessibility to data stored by public entities and that public information is availed via established channels in an accessible and safeguarded manner.

The master plan's first pillar is anchored on electronic government services, whose objective is to provide e-government services and information that is essential to improve efficacy, productivity and effective governance in every important industry segment. The second pillar is ICT as an industrial engine, which aims at transforming the main economic sectors of the Vision 2030 to considerably improve competitiveness at the global level, productivity and advancemet. The third pillar has to do with development of ICT enterprises that are capable of generating wealth and / or providing quality services and goods, comparable to those offered globally and that can therefore be placed on the export market. Electronic government services guarantees delivery of e-government data and products that are essential for the overall enhancement of the efficacy, productivity and management in every important area. [284]

The master plan goes further to identify integrated ICT infrastructure, and more specifically providing safe, reliable and cost effective connections throughout the country, as an important area of focus in the quest for the above broad objectives. Towards this end, it outlines a number of strategies among them being promotion of all-encompassing broadband connection by encouraging mobility of infrastructural resource providers to commission low cost last mile connections and developing, implementing and institutionalizing cyber security management framework.[285] Through the plan, the Government particularly targets facilitating the formation of suitable regulatory and organizational framework to protect applications, data resource and infrastructure. The Government also targets implementation of a cyber-security plan with a view

[284] Kenya ICT Authority. *Kenya National ICT Master Plan*. (Nairobi: 2013), 13.
[285] Ibid. 60.

of boosting ICT enabled economic development. This is to be achieved by way of offering user trust and assurance on available provisions including e-product exchange, national payment channels and overall safety of the cyber space. [286] The plan further targets enhanced integrity of public information that fosters efficient and effective service delivery, improved global ranking of the country on e-Government services by as a minimum fifteen places as well as improved accountability and transparency by ensuring secured accessibility to public information, consequently promoting the country's image internationally.

(d) National Cyber Security Strategy

Under this Strategy, cyber security is considered an important component as it provides individuals and corporate entities with improved confidence on internet based and electronic transactions, enabling higher volumes of direct investment by foreign entities as well as creating room for a broader collection of business opportunities on the global market. [287] To propel government cyber security commitment, the Strategy spells out four strategic goals. [288] The first goal is to enrich the country's cyber security position in a manner so as to facilitate national prosperity, security and growth. The second goal is to create national capacity through increased cyber security awareness and empowering the workforce to tackle requirements of a safe cyber space. The third goal is to nurture information exchange and cooperation amongst stakeholders thereby enabling a data sharing landscape that emphasizes on the fulfillment of the strategic objectives. The fourth goal is to deliver nationwide stewardship through definition of cyber security vision and purpose and coordination of cyber security programmes around the country.

[286] Kenya ICT Authority. *Kenya National ICT Master Plan*. (Nairobi: 2013), 60
[287] Ministry of Information, Communication and Technology. *National Cyber Security Strategy*. (Nairobi: MICT, 2013), 5.
[288] Ibid., 6.

The strategic objective defined under enhancement of the country's cyber security posture is that of protecting critical information infrastructure. This entails increasing security and resilience of infrastructure in order to safeguard government installations, residents and citizenry from cyber risks and realize socio-economic merits of the cyber environment. This is to be pursued through a coordinated mechanism with partner states to elevate global cyberspace security in its entirety and it encompasses safeguarding vital infrastructure, services and applications. It also involves joining hands with applicable stakeholders to develop cyber security capacities with specific emphasis on infrastructure, operations and mission assurance. The Strategy thus underscores the need for a managerial and institutional structure that will positively reinforce the cyber security features within both private and public spheres of the national economy.

There are two strategic objectives under building national capability, namely, training and awareness creation and roll-out of communications and outreach programmes. Under this goal, the Strategy aims to work with the academia in the development of cyber security higher education curricula as well as dedicated courses to breed competence amongst cyber security authorities.[289] It also targets creating, commissioning and upholding focused awareness creation programmes to enlighten both the workforce fraternity and members of the public at large of emerging cyber security risks and mitigation strategies. In this regard, it projects increased cyber threat understanding and empowering citizens to embrace safe online practices.

Information exchange and collaboration entails developing a comprehensive management model to guarantee prudent application of resources, reduced replication of effort and associated

[289] Ministry of Information, Communication and Technology. *National Cyber Security Strategy*. (Nairobi: MICT, 2013), 7.

conflicts and strive towards fulfillment of the country's long-range cyber security objectives. Specific activities relating to this goal include developing legislations as well as regulatory and policy instruments needed to safeguard the country's cyberspace, soliciting stakeholders' responses and contributions using appropriate methodologies and striking a balance between data security, confidentiality concerns and economic advancement priorities. [290]

The strategic objective under provision of national leadership is that of formulating and monitoring execution of the national Cyber Security Strategy as well as country specific Master Plan. It encompasses continued refreshing of the Strategy as may be necessary and establishing a premeditated action plan for attaining nationwide cyber security aims. It also envisages utilization of the Strategy and corresponding Master Plan to isolate and instigate appropriate cyber security programmes, in association with relevant stakeholder categories.[291]

(e) National ICT Policy

The policy is based on Vision 2030 and provides strategies necessary for attaining national development targets. The overarching aim of this policy is to help the government ensure that the entirety of the public service is strengthened via the deployment of high-quality ICT resources.[292] This includes reinforcement of service delivery systems within the education, health and infrastructural development segments of the economy. The broad strategies spelt out therein include promoting investment in the ICT sector, providing ICT training of relevant public sector

[290] Ministry of Information, Communication and Technology. *National Cyber Security Strategy*. (Nairobi: MICT, 2013), 8.
[291] Ibid.
[292] Ministry of Information and Communication. *National Information Communication and Technology Policy*. (Nairobi: MICT, 2016), 2.

service providers and employees, facilitating IT-oriented service delivery mechanisms in education, infrastructure and healthcare, facilitating employment of extensive internet applications, that is, remote sensors and management of linked instruments for environmental management and public utilities and inspiring institutions of higher education to upgrade learning systems and develop IT based learning solutions, for instance, by way of business sector partnerships. [293] In terms of infrastructure access, the policy underscores that increased incorporation of internet centered and other ICT associated provisions calls for suitable infrastructural resources in order for socio-economic advancement to gain root. It also acknowledges the fact that a strong IT resource base reinforces sustained progression for the ICT industry. Ultimately, it stipulates that the state machinery will continue promoting accessibility to as well as availability of dependable, affordable and efficient ICT infrastructure at both County and National levels of Government. [294] It particularly states that the Government will support construction of next-generation high-speed, mobile, secure and ubiquitous IT infrastructure, development of a modern industrial internet system, implementation of a national big data strategy and enhancement of IT security.[295] It further specifies that in order to develop up-to-date network systems, the government will put in place an elaborate action plan focused towards integrating big data, mobile internet, cloud computing as well as internet of things with emerging manufacturing trends; fostering e-commerce, internet banking, industrial internet and an advanced system that supports employment of high end technological applications in the agricultural, energy, tourism and financial services sectors as well as in managing logistics and other related public services. In addition, the necessary facilitation will be provided to internet-oriented firms in order to increase their visibility on the global landscape. This serves to provide

[293] Ministry of Information and Communication. *National Information Communication and Technology Policy*. (Nairobi: MICT, 2016), 14.
[294] Ibid.
[295] Ibid., 2.

and deploy adequate internet capabilities to basic education facilities, institutions of higher learning and commercial ventures as well as effective, reliable and safe internet resources.

Paragraph 15 of the policy provides that the state will establish and maintain a safe cyber-law environment, to reinforce the existing regulatory frameworks. Policy goals include establishment of a sufficiently empowered agency to handle cyber security, pursuit of emerging national cyber safety approaches with the aim of propelling both social and economic progression whilst also guarding internet dependent formations against cyber risks, promotion of new technological trends that culminate into reliable, quantifiable, available, safe and sustainable computer and IT systems and related governance and regulatory instruments that facilitate successful employment of new technology and advancement of data security standards for the IT industry that are to be taken up and utilized by the state entities and suggested to the private world as the best approaches. Policy objectives also include putting in place suitable regulatory and legislative machinery, technical innovations, policy enforcement schemes where both intelligence-linked and diplomatic mechanisms will be introduced as necessary in detecting and preventing cyber risks considering the extra territorial characteristic of these risks. The policy acknowledges that susceptible persons, for instance, children will need specific attention to guarantee their safety and source value from the cyber environment. It underscores the need for the delicate act of swift and effective mitigation of cyber risks in a bid to foster confidence and trust with the aim of safeguarding the internet platform openness as a new source of growth and innovation.[296] It further highlights the need for the establishment of a facilitative legislative instrument and cultivation of skills within not only the police but also the judiciary system, in conformity with the constitutional requirements, the dynamic regulatory and legislative

[296] Ministry of Information and Communication. *National Information Communication and Technology Policy*. (Nairobi: MICT, 2016), 21.

environment and consistent with the global and regional benchmarks and ensuring that the country is free from the cyber-crime menace.[297] Sub-paragraph 15.4 specifically addresses the question of security of information assets and it provides that the state will institute data security regulations and directives in order to protect the integrity, availability and confidentiality of information in accordance with Articles 31 and 35 of the Constitution. [298]

Through the policy, the Government also recognizes the value of data centres across all economic sectors and accordingly outlines strategies for effective utilization of data centres. These include a requirement for MDAs to jointly utilize and make optimal use of the data centre IT infrastructure so as to cut costs of having individual entities putting up their own infrastructure and also provide an extensive, cost-effective yet safe environment for state information. It also points out the need to ensure that Government information security is synchronized and managed centrally.[299]

4.2.3 Implementation of Principles of Information Security Through Performance Contracting Guidelines

The requirement for MDAs to implement the ISO 27001:2013 ISMS standard was incorporated in the performance contracting guidelines with effect from the 2016/2017 performance contracting period. Under the 13th cycle guidelines, issued in June, 2016, MDAs were required to undertake activities relating to security and safety of personnel, information and physical assets including documents and equipment. The MDAs were particularly expected to, among others,

[297] Ministry of Information and Communication. *National Information Communication and Technology Policy*. (Nairobi: MICT, 2016).
[298] Ibid.
[299] Ibid., 17.

institute strategies to control and manage technological exposures, terrorist strikes, natural calamities and fire and also implement the ISMS including training officers on the system.[300] The specific measures outlined in the performance contract guidelines towards implementation of the ISMS are as follows :

(a) Appoint ISMS leader
(b) Appoint and train ISMS champions
(c) Define scope
(d) Brief top management on ISMS
(e) Train implementers (process owners)
(f) Conduct awareness training for all staff
(g) Create ISMS Risk Management (Risk Registers and Risk Management Action Plan
(h) Finalize documentation of ISMS i.e. policy procedures and launch the ISMS based on the standard (ISO/IEC 27001)

The guidelines also required MDAs to undertake comprehensive measures towards automation of operations. This entailed assessing the level to which an MDA kept pace with developments and leveraged ICT in its business and service processes. The thrust of this indicator was holistic approach to ICT development as a package of improvement of speed and quality of service delivery, rather than siloed departmental activities. Key milestones to measure the indicator included development of institutional strategy and vision on ICT, installation of connectivity and technology infrastructure, consumer and business adoption including automation of essential public services, capacity building in ICT and adoption and compliance with ICT and e-

[300] Republic of Kenya. *13th Cycle Performance Contracting Guidelines*. (Nairobi: Performance Contracting Department, 2016), 13.

Government standards.[301] Most of the above provisions were retained in the performance contract guidelines for the subsequent years. The 15th cycle (2018/2019) guidelines go further by requiring MDAs to specifically establish information assets and secure them.[302] The MDAs are advised to determine information assets to be secured, inter alia, with reference to the importance, value, confidentiality, integrity and authenticity.[303]

The study revealed that on the overall, most MDAs are at the initial stages of implementing the ISO/IEC 27001 standard and that the standard is being implemented progressively by MDAs based on availability of resources and defined milestones for the individual institutions. Key challenges in implementing the standard include inadequate personnel to perform ISMS stewardship tasks on top of their daily job activities, financial resource constraints, lack of ownership and support across the board, limited awareness amongst staff on ISMS and data security and entrenched organizational culture. Other challenges include availability of several legal and policy instruments, multiplicity of actors, coordination gaps and the fact that ISMS monitoring and evaluation framework is not fully embedded amongst all MDAs. It was further noted that the security mechanism currently in place amongst the MDAs is largely based on specific initiatives as derived from the various Government legal and policy instruments explained above.

[301] Republic of Kenya. *13th Cycle Performance Contracting Guidelines*. (Nairobi: Performance Contracting Department, 2016), 13.
[302] Republic of Kenya. *15th Cycle Performance Contracting Guidelines*. (Nairobi: Performance Management and Coordination Office, 2018), 35.
[303] Ibid.

4.3 THE ROLE OF ISMS IN KENYA'S DEVELOPMENT AGENDA

Gboyega (2003) defines development as a phenomenon that covers all efforts to advance the quality of human lives in all situations.[304] It denotes enhancement of the overall welfare of every citizen, and not just the influential and wealthy, in a viable manner, such that the current consumption activities do not endanger the future. Additionally, it requires that poverty as well as skewed accessibility to necessities in life is eliminated or drastically reduced. It further entails improvement of individual physical security as well as the maintenance and broadening of life opportunities.

National development is a holistic approach that encompasses every facet of the life of an individual and the country. It has to do with reconstruction and advancement in various dimensions of a nation. It includes full-growth and expansion of various areas of the economy including manufacturing, education and agriculture as well as cultural, religious and social institutions. It deduces advancement of a country in totality. In the words of Bhawna Bawa, the concept refers to the all-inclusive and reasonable growth of diverse facets of the state, namely, socio-economic, cultural, social, political, material and scientific aspects.[305]

Naomi (1995) states that development entails economic growth and equity in the distribution of resources, health service provision, education, housing, among other major services aimed at enriching the quality of both individual and communal life. Chrisman (1984) considers

[304] A. Gboyega. Democracy and Development: *The Imperative of Local Governance*. An Inaugural Lecture, (University of Ibadan, 2003), 6- 7.
[305] Bhawna Bawa. *National Development: Meaning and Problems*. http://www.yourarticlelibrary.com/society/national-development-meaning-and-problems/76824/

development as a social progression process in which the improvement of individuals' wellbeing is achieved by strong ties between different industry players including institutional entities and other interested formations within the society.[306] He further asserts that development is not just an economic concern, but also entails social and political matters and encompasses all spheres of the society. It is an occurrence that covers the entire nation. National development can thus be explained as general enhancement or collective religious, economic, political and social progress of a country. This progress is best attained via development planning that may be discerned as national collection of approaches identified by the state.

Ebeh Igbogo (2015) advances the position that national development pertains to continuing depiction of positive modifications in the industrial, economic, cultural, industrial, political, administrative and social domains of a nation.[307] He further intimates that in examining a nation's progress, the concept national development is more encompassing as compared to that of economic growth. It entails large quantity and high value productive resources and their efficient utilization. When discussing national development, the key concern is on quality expansion in diverse areas of national existence, for instance, the social, psychological, political, economic, as well as ethical aspects of national existence.[308] These aspects supplement each other in the definition and assurance of productive and quality existence for the nation's citizens. It denotes political, cultural, economic, administrative, social and industrial transformation within an environment that is considered favourable and desirable for the realization of progress of civilization. The consistent and collaborative endeavour by citizens to apply the forces of

[306] O. Naomi. *Towards an Integrated View of Human Rights*. Hunger Teach Net, 1995, 6-7.
[307] Ebeh, John Igbogo. *National Security and National Development: A Critique*. International Journal for Arts and Humanities. Vol. 4(2), S/No 14, April, 2015, 3.
[308] Ibid.

nature as well as human potential for the general welfare of the citizenry is considered the most critical element in the discourse of national development.[309]

Igbogo also observes that national development and national security are two sides of the same coin. He further cites Egwu (2000) who, while analyzing causes of security challenges in Nigeria, observed that the security calculus of Nigeria State failed due to its failure to incorporate critical features of national and social development, for instance, provision of fundamental social services. The Nigerian government was, therefore, unable to satisfy not only the economic and social but also the military requirements for the country's security. Clearly, these challenges depict the failure by the government to consistently commit and sustain the key social virtues and physical resources for launching and maintaining the security of the nation, state survival as well as political and social betterment of the state.[310] Nwakpa (2000) reiterates the above position by stating that the rising national degeneration and insecurity instances is manifested in the retrogressing economy, deficient health care and health facilities, transport and water problems, fuelling challenges, high unemployment rate and other setbacks experienced by the Nigerian society.[311] From the above, it can be deduced that security is grounded on national development. Equally, the attainment of development could be attributable to a secure environment. For example, in violent situations such as ethnic clashes, destruction of infrastructure including electric poles and pipes, criminal acts like kidnap and robbery, among other grave offenses, have

[309] Ebeh, John Igbogo. *National Security and National Development: A Critique*. International Journal for Arts and Humanities. Vol. 4(2), S/No 14, April, 2015.
[310] Samuel Egwu. *The Origin, Nature and Politics of the Niger-Delta Crisis: The Consequences of Violence on the Future Youths*. A Paper Presented at a Workshop on the Reorientation of Youth for the Cause of Peace and Democratic Stability in the Niger-Delta, May, 2000.
[311] E. Nwakpa. *National Bar Association, Deplorers National Decay, Insecurity*. The Guardian, Friday, 1 October. 2000

impeded growth in foreign direct investment as well as expansion of infrastructural installations. It is, thus, evident that the two variables cannot be separated.[312]

As observed earlier, the Vision 2030 is Kenya's long-term growth plan that seeks to convert the nation to an industrialized, middle-income nation that offers high quality of life to every citizen in a secure and clean surrounding. The Vision consists of three core pillars, namely, economic; political and social. The economic pillar targets attainment of an annual economic growth rate of ten per cent and maintaining the same trajectory to 2030. The political pillar seeks to actualize an issue-oriented, individual-based, result-focused and a democratic system that is accountable whilst the social pillar aims to stimulate equitable, just and cohesive social advancement in a secure and clean setting. The three pillars are anchored on seven strategic enablers and these are science, technology and innovation, macroeconomic stability; security, infrastructural development, human resource development, land reforms and public sector reforms.[313] The Vision envisages establishment of an efficient, motivated and well-equipped public service as a fundamental ingredient of development.[314] It specifically focuses at building a public sector that is more citizen oriented as well as result based. In this regard, the Vision acknowledges ICT as the foundation for increased productivity of the public service and ultimately economic development. Through a knowledge based economy, the country's industrial development trajectory is focused on innovation whereby the adaptation, generation as well as application of knowledge remains a vital source of economic expansion. ICT is particularly a crucial component in the enhancement of human skills. Development of human capacity relies heavily

[312] Ebeh, John Igbogo. *National Security and National Development: A Critique*. International Journal for Arts and Humanities. Vol. 4(2), S/No 14, April, 2015. p 5
[313] Republic of Kenya. *Kenya Vision 2030*. (Nairobi: Government Printer, 2007), 6.
[314] Ibid., 9.

on a knowledge and information production, sharing and application system that consequently plays a prominent part in propelling production as well as economic growth.

The efficacy of a country's public sector is vital to actualizing the national vision and attendant development objectives. A proficient public sector enables not only delivery of quality services but also realization of set targets. Public servants are crucial in their role as policy designers, gatekeepers, distributors and administrators. Moreover, as a bridge between the wider public and the political class, public servants are critical in guaranteeing state permeation at the grassroots, apportionment and sharing of resources as well as implementation of set guidelines and rules. According to the UN Report, 2005, regardless of organization and constitution of government, it would be quite difficult to achieve much without a public administration system that can translate broad political intentions, enforce laws and deliver essential services to the people. [315] It further states that in the absence of professional competent public administration, the government cannot actualize its strategies or pre-empt undesirable developments. [316] In his contribution to the discourse, Prof. Joseph Ayee (2015) observes that public sector reforms have emerged as a staple of development in the developing economies including Africa and that efforts directed at public service reforms within the international community attest to the important role played by the public service.[317] He concludes by avowing that the public service

[315] United Nations Organization. United Nations Economic and Social Council Report, 2005. http://unpan1.un.org/intradoc/groups/public/documents/un/unpan021179

[316] Ibid.

[317] Prof. Joseph R.A. Ayee. *Public Sector Reforms in Africa*. Paper Presented at Commonwealth Association of Public Administration and Management Forum, 2015. https://www.capam.org/offerings/articles/2015/public_sector_reforms_in_africa.html (Accessed on April 25, 2018)

plays a central role in the growth of the nation and that its relevance cannot, therefore, be underestimated in Africa.[318]

The Kenyan public service comprises of the mainstream national government institutions, county governments and public corporations/state corporations. To attain operational efficacy it is necessary for the service to, among others, maintain high quality of service delivery, strengthen systems management as well as Government processes and promote leadership and administrative capacity of the public sector. Through the various MDAs, the Kenyan public service, contributes to national development in a couple of ways. First and foremost, the public service is the engine that propels the Government's development agenda. It supports government in creating an enabling governance framework/climate upon which the wealth of the nation depends. This includes national security and stability, peace, effective macro-economic management, conformity to legal processes and adherence to property rights, which are preconditions for development. The public service also ensures establishment, provision and maintenance of public goods which individual non-state actors cannot provide on their own, that is, products and services required for a nationally competitive production systems beyond the individual economic agents capacity – education, water and sewage, energy, transportation and communication network, In addition, the public service facilitates actions of economic agents, including individuals, private sector, Non-Governmental Organizations and development partners by providing services that directly impact the environment for non-state actors, such as, registration of companies, tax administration and spearheading public-private-partnerships.

[318] Prof. Joseph R.A. Ayee. *Public Sector Reforms in Africa*. Paper Presented at Commonwealth Association of Public Administration and Management Forum, 2015. https://www.capam.org/offerings/articles/2015/public_sector_reforms_in_africa.html (Accessed on April 25, 2018)

From the foregoing, it is evident that the public service is a linchpin of national development for it facilitates good governance framework, efficient public products and services and competitive national environment for non-state actors through policy formulation, implementation, enforcement and monitoring. This is, however, fortified by transformational national leadership that puts in place major institutional vehicles to deliver development and powerful agencies to prepare national development plans and coordinate their implementation. Through the implementation of ISMS the public service is facilitated in terms of maintenance of appropriate systems thereby contributing towards enhanced productivity and ultimately towards delivery of the development targets. Considering the fact that national development is predicated on efficiency and effectiveness in public service delivery, innovation is the heart of the public sector and the sector's ability to contribute to national development is, therefore, dependent on how well it leverages on research and ICT for enhanced efficiency, transparency and accountability. The ISMS makes it easier for the public service to manage for results in terms of assessing organizational capacity, mapping out of risk areas, managing security of information assets and implementation of other related targeted measures. This in essence complements realization of defined MDA mandates and by extension feeds into Kenya's national development planning.

3.5 CHAPTER SUMMARY

This chapter has assessed various legal and policy instruments that have been instituted in Kenya to address matters regarding information security. The laws evaluated include the Access to Information Act, 2016, the Computer Misuse and Cyber Crimes Act, 2018, the Critical Infrastructure Bill, 2015 and the Kenya Information and Communication Act, 1998 (Revised 2015). Policy instruments evaluated include the Ministry of ICT Strategic Plan (2013 – 2018),

the Kenya ICT Authority Strategic Plan (2013 – 2018), the Kenya ICT Master Plan (2013/14 – 2017/2018), the National Cyber Security Strategy and the draft National ICT Policy. The chapter has further assessed the level of implementation of ISO standard on ISMS amongst Kenya's public sector organizations and the place of information security and ISMS in Kenya's development agenda. Key observations and conclusions arising from these assessments are addressed in the next chapter.

CHAPTER FIVE

SUMMARY, CONCLUSION AND RECOMMENDATIONS

5.1 INTRODUCTION

This chapter consolidates pertinent issues arising from the previous chapters on the three study objectives. In this regard, the chapter presents a summary of study findings including key observations. It also provides conclusion and recommendations deriving from the study.

5.2 SUMMARY AND DISCUSSION

The first objective of this study was to explore key issues and factors influencing an effective ISMS. Towards this end, the study considered crucial areas of application of information technology and information security trends in Africa. The study also focused on the significance of safeguarding information assets and the principles and requirements for the introduction and maintenance of ISMS amongst Africa's public sector institutions. It further focused on the main information security governance practices and the specific requirements for the ISO/IEC 27001:2013 information security standard including the scope of the standard and steps to certification. Finally, it identified the benefits of not only maintaining ISMS but also of being ISMS certified. Arising from the data collected, it was established that being a risk based approach, the ISMS is a systematic way of managing prevalent information security risks thereby ensuring safety and availability of an organization's information assets. It was particularly noted that whereas most organizational entities possess some form of information security controls,

without an ISMS, the security control mechanism is mostly disjointed and disorganized. ISMS therefore provides an avenue for an all-inclusive approach to management of information assets where physical security, business continuity planning and information security are jointly managed while human resource practices entail definition and assignment of information security responsibilities throughout the organization. The study also established that modalities for implementing the ISMS vary amongst different corporate entities based on the complexity and unique circumstances surrounding the operations of individual organizations. Nevertheless, irrespective of the organization, successful implementation of ISMS requires commitment from the highest level and that as such it is very important for the top leadership of an organization and other major stakeholders to be duly sensitized of the necessity for information security. In addition, an effective ISMS requires, among others, analysis of security requirements for each information resource and application of appropriate controls to ensure protection of those assets, continuous evolution and adaptation to the changing technical landscape and policies and processes that protect an organization from misuse of data. The study further established that ISMS presents organizations with massive benefits and opportunities to leverage performance. These include safeguarding an organization's information assets, protection against cyber-attacks and other related risks, building synergy amongst an organization's functional units, enhancing productivity, increasing reliability and security of an organization's systems and enabling an organization to operate efficiently and effectively in the rapidly changing global environment. Finally, the study established that ISMS certification enhances an organization's corporate image thereby making it attractive to potential customers and other stakeholders.

The second objective was to evaluate Kenya's institutional and policy framework on information security and ISMS. The study revealed that Kenya has an elaborate institutional arrangement on

information security and ISMS and that the lead agencies in the implementation of information security strategies in the public sector are the Ministry of Information Communication and Technology and the Kenya ICT Authority of Kenya. The Ministry's involvement is at policy level in terms of development and overseeing implementation of appropriate policies and guidelines on ICT including information security policies. The Kenya ICT Authority is, on the other hand, mandated with establishing, maintaining and perfecting secure ICT systems and infrastructure including enforcing ICT standards and guidelines in the public sector through the various Government Ministries, Departments and Agencies. The study further established that the Government of Kenya has developed a number of legislations and policy documents touching on ICT, the main policies being, the Kenya Vision 2030, the Ministry of ICT Strategic Plan, the Kenya ICT Authority Strategic Plan, the Kenya National ICT Master Plan, the National Cyber Security Strategy and the National ICT Policy. To this end, it was noted that there is no stand-alone policy instrument on information security and ISMS and that matters concerning information security are embedded in an assortment of policy instruments.

The third study objective was to assess the extent and effect of application of ISMS standards in the Kenyan public sector policy environment. As indicated earlier, the study established that there is no stand-alone policy on ISMS. It was, however, noted that aspects of information security and ISMS have been captured under various legislative and policy frameworks. The key legal instruments where issues relating to information security have been highlighted include the Access to Information Act, 2016, the Computer Misuse and Cyber Crimes Act, 2018 and the Kenya Information and Communication Act 1998 (Revised 2015). These instruments specifically address matters concerning access to information, interruption, disruption or interference with computer system and management of records. They could, therefore, be

associated with ISMS requirements regarding control of access, suitable maintenance of records and managing data security related incidents. In terms of policy, the National ICT policy formulated by the Ministry of Information, Science and Technology underscores the significance of enhancing IT security as a panacea to attaining overarching national development objectives. The Kenya ICT Authority strategic plan (2013 – 2018) has on the other hand captured information security among the five key areas of strategic focus. This component entails development and incorporation of information security standards and guidelines, implementation of national cyber security master plan and strategy, strengthening the information security function within the ICTA, instituting a risk assessment and evaluation mechanism and undertaking periodic risk assessment on national information infrastructure. The cyber security strategy has since been developed in addition to an ICT master plan with a view to realizing the envisioned strategic objectives. The above policy interventions resonate well with ISMS provisions for planning, support and operation of information security system.

More importantly, the study established that with effect from 2016, through the issuance of performance contracting guidelines, the Government made it a requirement for all MDAs to implement ISMS in line with the ISO/IEC 27001:2013 standard. The MDAs were specifically required to build the necessary capacities and move progressively towards full implementation of the standard and ultimately certification. From the interaction, it was noted that most MDAs are still at the initial stages of implementing the standard in terms of appointment of ISMS leader, appointment and training of ISMS champions, defining scope and awareness training for employees. It was further noted that the main challenges encountered in implementing the standard include, inadequate personnel to perform ISMS tasks alongside their normal duties,

financial resource constraints, lack of ownership and support across the board, limited awareness amongst staff on ISMS and data security and entrenched organizational culture.

It is anticipated that full implementation of ISMS will strengthen service delivery systems thereby contribute towards a proficient Kenyan public sector and ultimately towards national development.

5.3 CONCLUSION

This research established that ISMS is a critical function of 21st century organizations in light of the incessant information security threats. The most pronounced threats include hackers, authorized insiders, cyber-terrorism and organized crime. The study has in this regard identified ISMS as an essential tool for organizations for purposes of securing their information assets. ISMS is not just confined to the security of computer devices. Rather, it is an integrated management system that is premised on a risk based approach aimed at collective response in securing information resources and realization of organizational objectives. Whereas the modalities for implementing specific aspects of the ISMS may vary from organization to organization, the study established that the underlying principles are the same. Key amongst these principles are awareness creation among staff, risk assessment for purposes of establishing risk portfolios and securing of top management commitment in the risk mitigation effort. In addition, the study established that ISMS encompasses individuals, IT systems and processes. It is a managerial structure that deploys a systematic business threat methodology in formulating, executing, operating, maintaining, overseeing, reviewing and enhancing the information security status of a corporate entity. ISMS implementation therefore calls for continuous review and

adaptation of the system so as conform to changes within the operating environment including the technical landscape. The ISO 27001:2013 ISMS standard was identified by the study as an approach that could be employed by public sector organizations within the African context for purposes of safeguarding information assets.

The issuance of Performance Contracting guidelines in 2016 with a requirement for all public sector institutions to incorporate ISMS within the performance contracting process demonstrates Government commitment towards implementation of the system. Most MDAs are currently in the process of building the necessary institutional capacities towards implementing the system. Besides, there is an indication of high level understanding of the requirements of ISMS within the policy and strategy formulation authority structure. The lack of a specific policy instrument on ISMS has, however, meant that Government initiatives on information security and ISMS are contained in a number of legislative and policy instruments which address different aspects of ISMS requirements. The attainment of the intended result also requires that the embedded challenges be addressed. This study contributes to both theory and practice of security management by demonstrating the interface between formal risk assessment and service delivery within the public sector setting.

5.4 RECOMMENDATION FOR FUTURE RESEARCH

This study was focused on examining key aspects of an effective ISMS and and the extent of application of ISMS standards within the Kenyan public sector policy environment. In this regard, limited attention was given to the actual implementation of ISMS requirements by

MDAs. A comprehensive study covering the implementation dynamics of the ISMS, including an in-depth analysis of challenges, resource impact and feedback is therefore recommended.

5.5 RECOMMENDATIONS FOR POLICY AND PRACTICE

ISMS is an aspect of the overall governance system of an organizational entity. The ultimate goal of ISMS is to protect an organization against information security risks and ensure orderly and structured approach to information management. Arising from the study findings, it is recommended that MDAs should invest in awareness creation of all staff on information security and ISMS. Top management commitment on ISMS should also be secured and upheld. Public sector institutions should further prioritize ISMS as an important ingredient in the fulfillment of their respective corporate mandates by incorporating it within their respective strategic planning frameworks. All MDAs should particularly strengthen their institutional capacities on ISMS by, among others, deploying adequate human and financial resources. Last but not least, the Kenya ICT Authority should consider developing an appropriate monitoring and evaluation mechanism so as to ensure timely implementation of the ISMS guidelines by MDAs. This may involve designing a suitable monitoring tool with specific timelines and providing strategic intervention procedures, where necessary.

REFERENCES

African Union Commission. *Agenda 2063: The Africa We Want*. (Addis Ababa: African Union Commission, 2015).

African Union Commission. *First Ten-Year Implementation Plan 2014 – 2023 of Agenda 2063*. (Addis Ababa: African Union Commission, 2015).

African Union Commission. *African Union Convention on Cyber Security and Personal Data Protection*, July, 2014. (Addis Ababa: African Union Commission, 2014).

Agosa Madiavale Beverly. *Information Security Management Practices and Organizational Goals: A Study of Microfinance Organizations In Nairobi*, Research Paper, University of Nairobi, October 2014.

Amarachi, A. A., Okolie, S. O., and C. Ajaegbu. *Information Security Management System: Emerging Issues and Prospects*. IOSR Journal of Computer Engineering, 2013.

Anderson, R. *Why Information Security is Hard-an Economic Perspective*. In Computer Security Applications Conference. New Orleans, Louisiana, 10th – 14th December, 2001.

Anie Sylvester O. Anie, *"Impact of Information Computer Technology on Primary Health Care Services to Rural Communities in Niger Delta Region of Nigeria*," Library Philosophy and Practice, 2011, http://www.questiaschool.com/read/1G1-260691387/impact-of-information-computer-technology-on-primary.

Appelbaum, S.H. *Social-Technical Systems Theory: An Intervention Strategy for Organizational Development*. Management Decision Journal, 35(6), 1997.

Babbie, Earl. *The Practice of Social Research. (*Belmont, CA: Wadsworth/ Thomson Learning, 2004)

Bacharach, S.B. *"Organizational Theories: Some Criteria for Evaluation,"* Academy of Management Review 14 (4), 1989.

Bawa, Bhawna. *National Development: Meaning and Problems*. http://www.yourarticlelibrary.com/society/national-development-meaning-and-problems/76824. Accessed April 10, 2018.

Blackwell E. *Building a Solid Foundation for Intranet Security*. Information Systems Management, Spring 15, 2, 1998.

Bostrom, R and Heinen, J. *Management Information System Problems and Failures: A Socio-Technical Perspective*. MIS Quartely Journal, September, 1977.

Braun, V. and Clarke, V. *Using Thematic Analysis in Psychology*. Qualitative Research in Psychology Journal, 2006, *3*(2).

Brewer, Peter C and Mills, Tina Y. "ISO 9000 Standards: An Emerging CPA Service Area," *Journal of Accountancy* 177, No. 2 (1994).

Bulgurcu, Burcu, Cavusoglu, Hasan and Benbasat, Izak. *Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness*. MIS Quarterly, Vol. 34, No. 3 (Management Information Systems Research Center, University of Minnesota, September 2010).

Cate H. Fred. *Information Security Breaches: Looking Back and Thinking Ahead.* (The Centre for Information Policy Leadership, Indiana University, 2008)

Cengage Learning. *Introduction to Information Security*. https://www.cengage.com/resource_uploads/downloads/1111138214_259146.pdf. Accessed March 20, 2018.

Cherdantseva, Y. and Hilton, J. "*The Evolution of Information Security Goals from the 1960s to Today*", Academic Paper Presented at Cardiff University, February, 2012.

Chetty, Lee-Roy. "*The Role of Science and Technology in the Developing World in the 21st "Century,"* Institute for Ethics and Emerging Technologies Journal, October 3, 2012.

Cichonski Paul et al. *Computer Security Incident Handling Guide*. (Gaithersburg: National Institute of Standards and Technology, 2012).

Cohen, A.B.J. and Nagin, D.(Eds.). *Deterrence and Incapacitation: Estimating the Effects of Criminal Sanctions on Crime Rates*. (Washington, DC: National Academy of Sciences, 1978).

Communications Authority of Kenya. *About Us*. On http://www.ke-cirt.go.ke/index.php/about-us. Accessed on 23rd March, 2018.

Communications Authority of Kenya. *Strategic Plan 2013 – 2018*. (Nairobi: Communication Authority, 2013).

D'Aiglepierre, Rohen et al. "*How Digital Technology Can Help Re-Invent Basic Education in Africa*." Quartz Africa Journal, November 13, 2017.

DeGarmo, Mathew T. Issues Concerning Integration of Unmanned Aerial Vehicles in Civil Airspace (McLean, Virginia: The MITRE Corporation, 2004).

Denning, D*., "Cyberterrorism",* Testimony Before the Special Oversight Panel of Terrorism Committee on Armed Services, US House of Representatives, 23 May 2000.

Denzin, Norman K. and Lincoln, Yvonna S. (Eds.). *The Sage Handbook of Qualitative Research*. (Sage Publications, 2017).

Dietz, Lawrence D. *Information Security Management in the 21st Century*. (California: Symantec Enterprise Security, 2013).

Dutta, Amitava and Roy, Rahul, "*The Dynamics of Organizational Information Security*" (2003). ICIS 2003 Proceedings. http://aisel.aisnet.org/icis2003/87. Accessed 18th March, 2018.

Dutta, Soumittra et al (eds). Global Information Technology Report, 2015 (Geneva, World Economic Forum, 2015).

Ebeh, John Igbogo. *National Security and National Development: A Critique*. International Journal for Arts and Humanities. Vol. 4(2), S/No 14, April, 2015.

Egwu, Samuel. *The Origin, Nature and Politics of the Niger-Delta Crisis: The Consequences of Violence on the Future Youths*. A Paper Presented at a Workshop on the Reorientation of Youth for the Cause of Peace and Democratic Stability in the Niger-Delta, May, 2000.

Evans, Lois. "Protecting Information Assets Using ISO/IEC Security Standards," *Information Management Journal*, November-December 2016.

Fielden, Kay. *An Holistic View of Information Security: A Proposed Framework*. International Journal for Infonomics *(IJI)*, Vol. 4, Issue 1, 2011.

Friedman, Bruce and Neuman, Karen Allen. *Systems Theory*. (In Theory and Practice in Clinical Social Work Practice edited by Jerrold R. Brandell, 2010).

Garbani, Jean-Pierre. *ISO, ITIL, COBIT: The Management Process*, CSO Journal, October 4, 2005. https://www.csoonline.com/article/2119437/data-protection/iso--itil--cobit--the-management-process-alphabet-soup.html

Gboyega A. *Democracy and Development: The Imperative of Local Governance*. An Inaugural Lecture, (University of Ibadan,2003).

Ghavifekr Simin and Rosdy W.A.W. *Teaching and Learning with Technology: Effectiveness of ICT Integration in Schools*. International Journal of Research in Education and Science (IJRES), 1(2), 2015.

Gianluca C. Misuraca. *E-Governance in Africa, from Theory to Action: A Handbook for Local Governance*. (Ottawa: International Development Research Centre, 2007).

Global Digital Forensics. Cyber Crime Forensics. https://www.iua.co.nz/site/iua/files/Cyber/Cyber%20Crime%20Terminology.pdf. Accessed April 6, 2018.

Gupta, M. *Activity Theory Guided Role Engineering*. Proceedings of 14th Americas Conference of Information Systems, Toronto, Canada, August 14-17, 2008.

Haubler Alexander. *ISO 27001: Information Security and the Road to Certification*. TUV SUD America, 2015.

Heyns, Report of the Special Rapporteur on Extrajudicial, Summary, or Arbitrary Executions, UN Doc. A/HRC/26/36, April 1, 2014; Ben Emmerson, Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, UN Doc. A/HRC/25/59, March 10, 2014.

Hormozi,Amir M., "Understanding and Implementing ISO 9000: A Manager's Guide," *SAM Advanced Management Journal* 60, No. 4 (1995).
http://www.yourarticlelibrary.com/society/national-development-meaning-and-problems/76824/

Igbogo Ebeh, John. *National Security and National Development: A Critique*. International Journal for Arts and Humanities. Vol. 4(2), S/No 14, April, 2015.

Indian Register Quality System. *Information Security Management System*. http://www.irqs.co.in/information-security-management-system.html. Accessed February 15, 2018.

International Organization for Standardization *Information Security Management Systems Requirements*. https://www.iso.org/standard/54534.html. Accessed March 20, 2018.

International Organization for Standardization ISO/IEC 27001:2013 Standard.

International Organization for Standardization. "ISO - ISO Standards - ISO/IEC JTC 1/SC 27 - IT Security Techniques".On https://www.iso.org/committee/45306/x/catalogue/.

International Organization for Standardization. *All About ISO*. https://www.iso.org/about-us.html. Accessed March 20, 2018.

International Organization for Standardization. *Information Security Management Systems*. https://www.iso.org/isoiec-27001-information-security.html. Accessed March 23, 2018.

International Organization for Standardization. *ISO in Brief*. (Geneva: ISO Central Secretariat, 2016).

International Organization for Standardization. *ISO/IEC 2700 Standards on Information Technology, Security Techniques, Information Management System Requirements*, 2005.

International Organization for Standardization. ISO/IEC 27001 International Standard.

International Public Sector Accounting Standards Board. *Key Characteristics of the Public Sector*. International Federation of Accountants, December, 2010.

Internet Society. Internet Infrastructure Security Guidelines for Africa. https://www.internetsociety.org/resources/doc/2017/internet-infrastructure-security-guidelines-for-africa/#_ftn1

ISO Certification. https://www.isoeasy.org. Accessed March 14, 2018.
Jansenn, Dale. *Hactivism*. https://www.techopedia.com/definition/2410/hacktivism. Accessed April 6, 2018.

Janssen Dale. *Security Breach*. https://www.techopedia.com/definition/29060/security-breach (Accessed on March 15, 2018)

Jaschob, Angelika and Tsintsifa, Lydia. IT-Grundschutz: Two-Tier Risk Assessment for a Higher Efficiency in IT Security Management. Information Security Solution Europe Conference, Rome, Italy, 2006, 95

Johnson Richard A., Kast Fremont E., and Rosenzweig James E. *Systems Theory and Management*. Management Science Journal. Vol. 10, No. 2, January, 1964

Johnson, Joseph et al., "A Comparison of International Information Security Regulations," *Interdisciplinary Journal of Information, Knowledge and Management* 9 (2014)

Jonscher, Charles, "Chapter 1 an Economic Study of the Information Technology Revolution," in *Information Technology and the Corporation of the 1990s: Research Studies*, ed. Thomas J. Allen and Michael S. Scott Morton (New York: Oxford University Press, 1994).

Kenya ICT Authority. *Kenya National ICT Master Plan*. (Nairobi: ICTA, 2013).

Kenya ICT Authority. *Strategic Plan, 2013 – 2018*. (Nairobi: ICTA, 2013).

Kimwele, M., Mwangi, W., and Kimani, S. .*Information Technology (IT) Security Management in Kenyan Small and Medium Enterprises (SMEs).* International Journal of Computer Science and Information Technologies, 2 (1), (2011).

Kisilu Donald and Tromp Delno. *Proposal and Thesis Writing* (Nairobi, Paulines Publication Africa, 2006).

Kitheka M. Philip. *Information Security Management Systems in Public Universities in Kenya; A Gap Analysis Between Common Practices and Industry Best Practices* (University of Nairobi, 2013).

Kittur, N. *Cognition, Computation, Design*. 2006. http://www.kittur.org. Accessed April 23, 2018.

Koch, Per. *The Difference Between Public and Private Sectors*. The Publin Post Newsletter, No. 7, 2005.

Kong, H., Jung, S., Lee, I., and Yeon, S. J. *Information Security and Organizational Performance: Empirical Study of Korean Securities Industry*. ETRI Journal, 2015, 428-437.

Kozmetsky George, Williams Frederick and Williams Victoria. *New Wealth: Commercialization of Science and Technology for Business and Economic Development* (Westport, CT: Praeger, 2004).

Kvochko, Elena. *Five Ways Technology Can Help the Economy*, World Economic Forum, 2013, https://www.weforum.org/agenda/2013/04/five-ways-technology-can-help-the-economy/

Kwankam, Yunkap S. *"What E-Health Can Offer,"* Bulletin of the World Health Organization, Volume 82, Issue No. 10 (2004).

Lankford, William M., "ISO 9000: Understanding the Basics," *Review of Business* Volume 21, Issue No. 1 (2000).

Larsen, H.M. Larsen, Pedersen, K.M. and Andersen K.V. *"IT Governance Reviewing 17 IT Governance Tools and Analysing the Case of Novozymes"* .Proceedings of the 39th Hawaii International Conference on Systems Science, 2006.

Laudon, K.C and Laudon J.P. *Management Information System*. (New Delhi: Pearson Education, 2016).

Liua, Chunlin et al. The Security Risk Assessment Methodology. International Symposium on Safety Science and Engineering in China, 2012.

Ma, Qingxiong et al., "An Integrated Framework for Information Security Management," *Review of Business* Journal, Volume 30, Issue No. 1 (2009).

Malik, Amitav. *Technology and Security in the 21st Century: A Demand-Side Perspective* (Oxford: Oxford University Press, 2004).

Markus, M.L., and Saunders. "Looking for a Few Good Concepts and Theories for the Information Systems Field," MIS Quarterly, 31 (1), 2007.

Masuti, Oliver. Impact of IT on Society in the New Century. http://www.zurich.ibm.com/pdf/news/Masutti.pdf. Accessed May 25, 2018.

Maumbe, Blessing M. International Journal of ICT Research and Development in Africa, http//: www. Igi-global.com, 2010. Accessed April 10, 2018.

McPhee, Ian. *"Risk and Risk Management in the Public Sector"*. Public Sector Governance and Risk Forum, September 1, 2005.

Mertens, D.M. *Inclusive Evaluation: Implications of Transformative Theory for Evaluation*. American Journal of Evaluation, 20(1), 1999.

Ministry of Information and Communication. *National Information Communication and Technology Policy*. (Nairobi: MICT, 2016).

Ministry of Information and Communication. *National Information Communication and Technology Policy*. (Nairobi: MICT, 2016).

Ministry of Information, Communication and Technology. *National Cyber Security Strategy*. (Nairobi: MICT, 2013).

Ministry of Information, Communication and Technology. *Functions of the State Department of Broadcasting and Telecommunication*. http://www.ict.go.ke/broadcasting-and-telecommunication/. Accessed June 20, 2018.

Ministry of Information, Communication and Technology. *Strategic Plan, 2013-2018.* (Nairobi: MICT, 2013).

Misuraca, Gianluca C., *E-Governance in Africa, from Theory to Action: A Handbook on ICTs for Local Governance* (Ottawa: International Development Research Centre, 2007).

Mody Bella, Bauer Johannes M., and Straubhaar Joseph D., eds., *Telecommunications Politics: Ownership and Control of the Information Highway in Developing Countries* (Mahwah, NJ: Lawrence Erlbaum Associates, 1995).

Naomi O. *Towards an Integrated View of Human Rights*. Hunger Teach Net, 1995, 6-7.
National Research Council. *Safe Computing In the Information Age.* (Washington: National Academy Press, 1991).

Naseba and Africa Cyber Space Network. *Africa Cyber Defence Summit*. https://www.eventbrite.com/e/africa-cyber-defence-summit-2018-nairobi-kenya-tickets-43780384308/, (Accessed June 23, 2018)

National Institute of Environmental Health Science. "Biomedical Information Science and Technology Initiatives," *Environmental Health Perspectives Journal.* Vol 108, Issue No. 11 (2000).

Negi, Yogita. *Pragmatic Overview of Hacking and Its Counter Measures*. Proceedings of the 5th National Conference, Bharati Institute of Computer Applications and Management, New Delhi, India, March 10 – 11, 2011.

Nurre Anthony, Gunaman Yusuf and De-Almeida Dennis. *What It Means to be ISO 9000 Certified*. Research Paper. September 22, 2000.

Nwakpa, E. *National Bar Association, Deplorers National Decay, Insecurity*. The Guardian, Friday, 1 October. 2000.

Odedra, M. *Information Technology Transfer to Developing Countries: Cases from Kenya, Zambia and Zimbabwe*. PhD Thesis, London School of Economics, September 1990.

Organization for Economic Co-operation and Development. *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*. (Paris: OECD, July 2002), www.oecd.org. Accessed March 20, 2018.
Oscarson Per. *Information Security Fundamentals*. (Orebro University, 2014).

Owiti, J. "*Information Security Management Present and Future*". ICPAK 27th Annual Seminar, 2011.

Park, C.S., Jang, S. S., and Park, Y. T. A study of effect of Information Security Management System [ISMS] Certification on Organization Performance. International Journal of Computer Science and Network Security, 2010.10 (3).

Perry Johnson Registrars Inc. *Information Security Management System*. http://www.pjr.com/standards/iso-27001/information-security-management-system (Accessed on March 24, 2018)

Prof. Adei, Stephen. *The Role of Public Service in a Developmental State: Lessons from the Newly Industrialized Countries (NICs) for Africa*. African Association For Public Administration and Management, 30th AAPAM Annual Roundtable Conference, Accra, Ghana 6th – 10th October 2008.

Prof. Ayee, Joseph R.A. *Public Sector Reforms in Africa*. Paper Presented at Commonwealth Association of Public Administration and Management Forum, 2015. https://www.capam.org/offerings/articles/2015/public_sector_reforms_in_africa.html. Accessed April 25, 2018.

Reich B.H. and Benbasat I. *Factors that Influence the Social Dimension of Alignment Between Business and Information Technology Objectives*, MIS Quarterly Journal, Vol 24, Issue No. 1, 2000.

Republic of Kenya. *13th Cycle Performance Contracting Guidelines*. (Nairobi: Performance Contracting Department, 2016).

Republic of Kenya. *15th Cycle Performance Contracting Guidelines*. (Nairobi: Performance Management and Coordination Office, 2018)

Republic of Kenya. *Access To Information Act No. 31 of 2016*. (Nairobi: Government Printer, 2016).

Republic of Kenya. *Computer Misuse and Cyber Crimes Act, 2018*. (Nairobi: Government Printer, 2018).

Republic of Kenya. *Kenya Information and Communication Act*. (Nairobi: Government Printer, 2015).

Republic of Kenya. *Kenya Vision 2030*. (Nairobi: Government Printer, 2007).

Richard Oppenheim, *"Technology Trends: Part 1: All the Time, Everywhere," Searcher*, May 2010, http://www.questiaschool.com/read/1G1-225589445/technology-trends-part-1-all-the-time-everywhere

Rogers, Yvonne Rogers. *A Brief Introduction to Distributed Cognition*. Interact Lab, School of Cognitive and Computer Sciences, University of Sussex, August, 1997.

Rouse Margaret. *Information Security*. http://searchsecurity.techtarget.com/definition/information-security-infosec (Accessed on March 15, 2018).

Salej, Stefan, Bogdan. *Models of the State Ownership Function Organization.* Proceedings of the High Level Meeting of State Ownership Authorities, 5th – 6th September, 2011, Ljubljana, Slovenia

Sanders, Ralph. *International Dynamics of Technology* (Westport, CT: Greenwood Press, 1983).

Schacter, Mark. Public Reforms in Developing Countries: Issues, Lessons and Future Directions. (Ottawa: Institute of Governance, 2002).

Serianu Research Team. Africa Cyber Security Report (Nairobi: Serianu Limited, 2016).

Shituma, Shikuku. *Adoption of Telemedicine in Hospitals in Nairobi County*. Research Paper Presented at the School of Business, University of Nairobi, November, 2013.

Singh, S., & Karaulia, D. S. *E-governance: Information Security Issues*. In Proceedings of the International Conference on Computer Science and Information Technology, 2011

Sirma, J., Muiru, M., and Kipchillat, D. C. *Impact of Information Security Policies on Computer Security Breach Incidences in Kenyan Public Universities*. Information and Knowledge Management Journal, Vol. 4, 2014.

Taskforce on Harmonization of Public Sector Accounting. *Government / Public Sector / Private Sector Delineation Issues*. Fourth meeting of the Advisory Expert Group on National Accounts, Frankfurt, 30 January – 8 February 2006.

The BSI Group. ISO/IEC 27001:2013 Implementation Guide. https://www.bsigroup.com/LocalFiles/en-GB/iso-iec-27001/resources/ISO-27001-implementation-guide.pdf. Accessed March 23, 2018.

The Institute of Internal Auditors. Supplementary Guidance: *Public Sector Definition*. December, 2011.

The Presidency. Executive Order No. 1 of 2018. (Nairobi: Government Printer, 2018).

Thor, Olavsrud Thor. Information Security Threats that will dominate 2018. Computerworld Philipines, Online Edition 1, Business Source Complete. Accessed June 1, 2018.

Tipton, Harold F. and Krause, Micki. *Information Security Management Handbook*. (London: CRC Press, 2004).

Tyler, M. Hughes, J. and Renfrew, H. *Kenya: Facing the Challenges of an Open Economy*. In E.M. Noam (Ed.), Telecommunications in Africa, (London: Oxford University Press, 1999).

UNESCO. *E-Learning: Promoting Distance Education at the Secondary Level, 2005*. http://portal.unesco.org/en/ev.phpURL_ID=28751&URL_DO=DO_TOPIC&URL_SECTION=201.html. Accessed May 10, 2018.

UNESCO. *e-Project ABC - Mobiles for Literacy*. Background Case Study authored for UNESCO by Christopher Ksoll in 2013. [Unpublished].

United Nations Organization. United Nations Economic and Social Council Report, 2005. http://unpan1.un.org/intradoc/groups/public/documents/un/unpan021179.

University of Michigan. *Standard Practice Guide Policies: Information Security Incident Reporting*, 2016.

Wafula, Paul. *Kenya To Set Up Unit to Protect Critical Infrastructure*. Standard Newspaper, Wednesday, 2nd September, 2015.

Waithaka, Francis. *Insights from Africa Cyber Security Report*. https://digital4africa.com/2018/04/20/insights-africas-cyber-security-report/ (Accessed June 23, 2018)

Wangwe, Samuel M., ed., *Exporting Africa: Technology, Trade, and Industrialization in Sub-Saharan Africa* (New York: Routledge, 1995).

Whitman, Michael E. and Mattord, Herbert. J. *Principles of Information Security*. (Boston: Cengage Learning, 2011).

Wong, Wilson S. *Emerging Military Technologies: A Guide to the Issues* (Santa Barbara, CA: Praeger, 2013).

World Bank. *African Development Indicators*, (Washington: The World Bank, 2007).

World Economic Forum. *The Future of Jobs and Skills*. (Geneva: World Economic Forum, 2016).

World Health Organization. "Emerging Science and Technology for Health," *Bulletin of the World Health Organization*, Volume 71, Issue No. 6, 1993.

Yonazi, Enock et al (eds). *Use of ICTs for Agriculture in Africa*. Joint Report By the African Development Bank, Korean Trust Fund, World Bank Pfizer Trust Fund and World Bank Africa Regional Department, 2012.

Zviran, M and Haga, W.J. Haga. Password Security: An Empirical Study. Journal of Management Systems, Vol. 5, Issue No. 4, 1999.

APPENDICES

Appendix 1

IMPLEMENTATION OF INFORMATION SECURITY MEASURES IN KENYA

KEY INFORMANT GUIDE

A. INTRODUCTION

The purpose of this study is to identify key issues and factors influencing an effective Information Security Management System and reviewing Kenya's institutional and policy framework on information security and ISMS. The study is also aimed at assessing the extent and effect of application of ISMS standards in the Kenyan public sector policy environment with a view to informing future policy decisions. You have been identified as one of the key informants in this survey. In this regard, it would be appreciated if you could enrich the research by responding to the following few questions to the best of your knowledge. The information provided will be used solely for academic purposes and all responses will be treated with confidentiality.

B. KEY INFORMANT'S BIODATA

1. Job Title and Job Group (where applicable)……..

2. Department/ Unit (where applicable)……

3. Scope of work (including duties and responsibilities)……..…….……

4. How long have you been in your current organization

   (a) Less than 1 year [ ]

   (b) Between 1 - 4 years [ ]

   (c) Between 5-9 years [ ]

   (d) 10 years and above [ ]

C. INSTITUTIONAL AND POLICY FRAMEWORK

5. What policies have been put in place by the Government to address issues of ISMS?

6. What is the role of your department/unit on matters regarding ISMS and IT security?

D. IMPLEMENTATION STATUS

7. How would you rate institutional capacities of Kenya public sector institutions in the rollout of ISMS under the following categories? (Very Strong, Strong, Average, Weak, Very Weak)

   (a) Policy Framework

   (b) Professionalism and Quality of Staff

   (c) Mechanism for Reporting and Managing ISMS Practices

   (d) Sensitization and Awareness Creation

8. In your own assessment, how widespread is use of ISMS amongst MDAs?

   (a)Almost all MDAs are involved in it [ ]

   (b) Most MDAs are involved in it [ ]

   (c)Only a few MDAs are involved in it [ ]

   (d) Hardly any MDA is involved in it [ ]

   (e)Don't Know/Not Applicable [ ]

9. How would you rate the level of IT security in Kenya today?

   (a)Very high [ ]

   (b) Moderate [ ]

   (c)Low [ ]

   (d) Don't know [ ]

D. EFFECTS

10. In your opinion what has been the effect of implementing ISMS in Kenya?

11. In what ways would you say ISMS contributes towards National Development?

E. CHALLENGES

12. What would you say are some of the major challenges encountered in the implementation of ISMS in particular and IT security systems in general amongst MDAs?

13. What measures have been put in place to mitigate some of the identified challenges?

F. FUTURE PROSPECTS

14. What are some of the future plans as far as implementation of ISMS in Kenya is concerned?

15. What areas would you want improved in order to effectively implement ISMS amongst the MDAs?

Thank you

Date _____

Appendix 2

CHECKLIST FOR KEY PROVISIONS FOR THE ESTABLISHMENT,

IMPLEMENTATION AND MAINTENANCE OF ISMS UNDER ISO/IEC 27001:2013

Item	**Areas of Focus**
Context of the organization	• Assessment of internal and external factors that could affect successful implementation of ISMS. • Specification of the scope of ISMS standard • Modalities for establishing, implementing, maintaining and continually improving the ISMS in relation to the standard
Leadership	• Formulation of an information security policy • Assignment of responsibility and authority to implement the policy • Active promotion of organization-wide understanding of the importance of information security
Planning	• Identification and assessment of information security risks • Identification of possible risk control mechanisms • Development of a treatment plan to address the risks. • Establishment of information security objectives
Support	• Provision of necessary resources to establish, implement, maintain and continuously improve ISMS. • Sensitization of all personnel on information security • Control of access to documented information
Operation	• Execution of information security policies, practices and processes • Maintenance of suitable records that document results • Conduct of performance assessments at planned intervals and implementation of the risk treatment plan
Performance Evaluation	• Monitoring, measurement, analysis and evaluation of ISMS at planned intervals to assess its suitability and effectiveness
Improvement	• Continual improvement • Identification of nonconformities • Taking corrective action to improve the effectiveness of the ISMS