

**A MODEL FOR DETERMINING INFORMATION SECURITY
PREPAREDNESS LEVEL IN E-GOVERNANCE IN KENYA'S COUNTY
GOVERNMENTS: CASE OF UASIN GISHU COUNTY GOVERNMENT**

KORIR GLADYS

**A Thesis Submitted to the Institute of Postgraduate Studies of Kabarak University
in Partial Fulfillment of the Requirements for the Award of Master of Science in
Information Technology**

KABARAK UNIVERSITY

NOVEMBER 2023

DECLARATION

1. I do by declare that:

- i. This thesis is my own work and to the best of my knowledge it has not been presented for the award of a degree in any university or college.
- ii. That the work has not incorporated material from other works or a paraphrase of such material without due and appropriate acknowledgement
- iii. That the work has been subjected to processes of anti-plagiarism and has met Kabarak University 15% similarity index threshold

2. I do understand that issues of academic integrity are paramount and therefore I may be suspended or expelled from the University or my degree may be recalled for academic dishonesty or any other related academic malpractices.

Signed:.....

Date:

Korir Gladys

GMI/ON/0143/01/16

RECOMMENDATION

To the Institute of Postgraduate Studies:

The research thesis entitled “**A Model for Determining Information Security Preparedness Level in E-Governance in Kenya’s County Governments: Case of Uasin Gishu County Government**” and written by **Korir Gladys** is presented to the Institute of Postgraduate Studies of Kabarak University. We have reviewed the research thesis and recommend it be accepted in partial fulfillment of the requirement for the award of the degree of Master of Science in Information Technology.

Signature:.....

Date:

Dr. Moses Thiga

Lecturer, School of Science, Engineering and Technology

Kabarak University

Signature:.....

Date:

Dr. Lamek Rono

Lecturer, School of Infocoms

Rongo University

COPYRIGHT

© 2023

Korir Gladys

All rights reserved. No part of this Thesis may be reproduced or transmitted in any form using either mechanical, including photocopying, recording or any other information storage or retrieval system without permission in writing from the author or Kabarak University.

DEDICATION

I am dedicating this thesis to family: Indeed, you have been a great source of inspiration to me and for the support you accorded me in every way you could.

ACKNOWLEDGEMENT

I thank the Almighty GOD for the far He has brought me. I express my sincere gratitude to my supervisors the late Prof. Kefa Rabah, Dr. Moses Thiga and Dr. Lamek Ronoh who greatly contributed in this work and for their guidance and patience throughout my thesis writing.

Additionally, I want to salute my friends and colleagues Sharon Kimutai, Zeddy Chelangat, Kenneth Biy, Evans Ombati, Joshua Mutai, Dorcas Chemjor and Bernard Bett for their insights during the course of writing my thesis.

My special gratitude goes to my dear family for their full time support in ensuring that I had all I needed.

ABSTRACT

The growing adoption of e-governance systems in Kenya's public sector is a testimony to its critical role as an effective tool for public service delivery. However, providing the public with information and services through e-governance systems, poses profound threats to security of information and citizens' trust in the ability of e-governance systems to secure their valued information. The main purpose of the study was to develop a model that can be used by governments to determine their preparedness level in protecting e-governance systems against information security threats. The objectives of the study were; to determine fundamental information security control measures that can be used in the development of the model, to develop the model, to implement and evaluate the model for determining organization information security preparedness level. The model utilizes a web-based platform containing specific information security indicators against which different departments dealing with information security can assess their capability to defend e-governance systems. The study adopted design science research and rapid prototyping methodology to develop and implement the model. The research target population were selected based on their knowledge, experience and roles in e-governance. The study adopted cluster and simple random sampling methods. Simple random sampling method was used to identify respondents in each cluster. To evaluate the model, a goal-based approach was used and validity test was conducted. The study established that while the government has invested heavily in technical information security measures, it has however failed to evaluate and perform a routine review of its information security practices. This research contributes to existing knowledge on e-governance security by providing a method by which governments can use to assess their information security practices. The model is recommended for use by key information security personnel in Kenya's county governments to assess their information security preparedness and hence work towards improving their organizational information security practices.

Keywords: *E-governance, Information Security, Information Security Control Measures, Organization Information Security Preparedness*

TABLE OF CONTENTS

DECLARATION	ii
RECOMMENDATION	iii
COPYRIGHT	iv
DEDICATION	v
ACKNOWLEDGEMENT	vi
ABSTRACT	vii
TABLE OF CONTENTS	viii
LIST OF TABLES	xii
LIST OF FIGURES	xiii
ABBREVIATIONS AND ACRONYMS	xiii
CONCEPTUAL AND OPERATIONAL DEFINITION OF TERMS	xv
CHAPTER ONE	1
INTRODUCTION	1
1.1 Overview.....	1
1.2 Background to the Study	1
1.3 Statement of the Problem.....	5
1.4 Purpose of the Study	6
1.4.1 General Objectives of the Study	6
1.4.2 Specific Objectives of the Study.....	6
1.5 Research Questions.....	7
1.6 Significance of the Study	7
1.7 Justification of the study	8
1.8 Scope of the Study	8
1.9 Limitation and Delimitations of the Study	9
1.10 Assumptions of the Study	10
CHAPTER TWO	11
LITERATURE REVIEW	11
2.1 Introduction.....	11
2.1.1 E-governance	11
2.1.2 A Review of E-Governance in Kenya	13
2.1.3 Information Security	16
2.1.4 Information Security Challenges Affecting E-Governance.....	19
2.2 Information Security Control Measures	23

2.3 Information Security Roles and Responsibilities	28
2.4 Information Security Assessment	28
2.4.1 Baldrige Cyber Security Excellence Builder (BCEB)	29
2.4.2 NIST Framework for Cyber Security Risk Assessing	30
2.4.3 Maryland Health Care Commission Cyber Security Assessment Method	31
2.4.4 FIFIEC Cyber Security Assessment Method	32
2.4.5 Information Security Risk Assessment	33
2.4.6 Fuzzy Theory Model for Assessing Information Security Controls	33
2.4.7 Data Protection Assessment Method	34
2.4.8 CS ² SAT: The Control Systems Cyber Security Self-Assessment Tool	34
2.5 Existing Frameworks	35
2.6 Summary of Existing Methodologies	45
2.7 Model Development Methodologies	48
2.8 Model Evaluation Methodologies	50
2.9 Theoretical Framework	52
2.9.1 Technological Controls	53
2.9.2 Organizational Controls	55
2.9.3 Environmental Controls	56
2.10 Research Gap	57
2.11 Conceptual Framework	58
CHAPTER THREE	61
RESEARCH METHODOLOGY	61
3.1 Introduction	61
3.2 Research Paradigm	61
3.3 Target Population	61
3.4 Sampling Procedure	62
3.4.1 Sample Size	62
3.4.2 Sample Technique	63
3.5 Research Instrument	63
3.6 Data Collection Procedure	63
3.7 The Pilot Study	64
3.7.1 Reliability Analysis	64
3.8 Data Analysis	65
3.9 Model Development	66

3.10 Model Evaluation.....	68
3.11 Ethical Consideration.....	69
CHAPTER FOUR	70
DATA ANALYSIS, PRESENTATION AND DISCUSSION	70
4.1 Introduction.....	70
4.1.1 Response Rate.....	70
4.1.2 General Background Information	70
4.2 Data Analysis.....	72
4.2.1 Technological Controls.....	73
4.2.2 Organization Controls.....	82
4.2.3 Environmental Controls.....	88
4.2.4 Information Security Preparedness Indicators.....	92
4.2.5 Correlation Analysis	94
4.2.6 Regression Analysis.....	95
4.2.7 Model Significance.....	96
4.2.8 Model Weights.....	97
4.3 Derivation of Relevant Weights	98
4.4 Model Metrics.....	100
4.4.1 Best Case Scenario	100
4.4.2 Worst Case Scenario.....	100
4.4.3 Threshold Scores	101
4.5 Model Implementation.....	101
4.5.1 Model Objectives.....	102
4.5.2 Model Requirements Specifications	102
4.5.3 Model Overview	103
4.5.4 System Contributors	104
4.5.5 OISP System Architecture.....	105
4.5.6 Proof of Concept.....	121
4.6 Model Evaluation.....	121
4.6.1 Model Validity.....	123
4.7 Scalability	125
CHAPTER FIVE	126
SUMMARY, CONCLUSIONS AND RECOMMENDATIONS	126
5.1 Introduction.....	126

5.2 Summary of the Major Findings	126
5.3 Conclusion	128
5.3.1 Fundamental Information Security Controls that can be used to Determine OISP Level in E-governance	129
5.3.2 OISP Model Development.....	129
5.3.3 OISP Model Implementation.....	130
5.3.4 OISP Model Evaluation.....	130
5.4 Recommendations.....	130
5.4.1 Policy Recommendation.....	130
5.4.2 Recommendation for Further Research	131
REFERENCES	132
APPENDICES.....	136
Appendix I: Questionnaire	136
Appendix II: Validity Tool.....	142
Appendix III: Research Letter	144
Appendix IV: University Research Permit.....	145
Appendix V: Introduction Letter	146
Appendix VI: NACOSTI Authorization Letter.....	147
Appendix VII: NACOSTI Research Permit.....	148
Appendix VIII: List of Publications	149
Appendix IX: Evidence of Conference Participation.....	150

LIST OF TABLES

Table 1: Information Security Controls	24
Table 2: Summary of Information Security Assessment Methodologies	46
Table 3: Target Population	62
Table 4: Reliability Analysis for the Pilot Study	65
Table 5: Job Title	70
Table 6: Highest Academic Qualification	71
Table 7: How long have you been Working for this county?	71
Table 8: Work Experience in Information Technology	72
Table 9: Access Controls	73
Table 10: System Software Security Safeguarding Measures	78
Table 11: Network Security and Server Security Safeguarding Measures	78
Table 12: Data Security Safeguarding Measures	80
Table 13: Human Resource Security Safeguarding Measures	80
Table 14: Information Security Policy	85
Table 15: Awareness Creation, Training and Education	87
Table 16: Compliance	89
Table 17: Physical and Environmental Security	91
Table 18: Information Security Preparedness Indicators	93
Table 19: Correlation Analysis Matrix	94
Table 20: Model Summary	96
Table 21: F-statistics	96
Table 22: Coefficients ^a	97
Table 23: Goal-Based Evaluation for the OISP System	122
Table 24: Validity Analysis	124

LIST OF FIGURES

Figure 1: Interaction between the Main Groups in E-governance.....	12
Figure 2: Information Security Model	18
Figure 3: Problem Space: Security Islands	20
Figure 4: Challenges in E Governance	22
Figure 5: Baldrige Cybersecurity Excellence Builder Components.....	30
Figure 6: PDCA Model.....	37
Figure 7: Components of NIST Cyber Security Framework.....	39
Figure 8: Core function of NIST Cyber Security Framework	40
Figure 9: COBIT 5 Principles.....	43
Figure 10: COBIT 5 Enablers.....	43
Figure 11: SDLC Activities	48
Figure 12: Design Science Research Process	50
Figure 13: Conceptual Framework	59
Figure 14: Architectural Framework	60
Figure 15: Rapid Prototyping Development Activities	67
Figure 16: OISP System Flowchart	104
Figure 17: Entity Relationship Diagram.....	108
Figure 18: Login Flowchart.....	110
Figure 19: OISP Login GUI	110
Figure 20: Self-Assessment Module.....	111
Figure 21: Self-assessment GUI.....	112
Figure 23: User Score Report GUI.....	114
Figure 24: Recommendation Reports GUI.....	115
Figure 26: OISP Users Score Report GUI.....	116
Figure 27: Setting GUI	116
Figure 28: User Registration GUI	117
Figure 29: New Role Registration GUI.....	118
Figure 30: All Questions Lists GUI.....	118
Figure 31: Add New Assessment Question GUI.....	119
Figure 32: Assigning Questions GUI	120
Figure 33: OISP Dashboard.....	121

ABBREVIATIONS AND ACRONYMS

BCEB	-	Baldrige Cyber security Excellence Builder
CISO	-	Chief Information Security Officer
COBIT	-	Control Objectives for Information and Related Technology
CSF	-	Cyber security framework
DSR	-	Design Science Research
GEA	-	Government enterprise architecture
ICT	-	Information and communication technologies
ICTA	-	Information and communication technology Authority
IDS	-	Intrusion Detection System
IFMIS	-	Integrated Financial Management information system
IPS	-	Intrusion Prevention System
IS	-	Information Security/System
ISMS	-	Information security management system
ISO	-	International Standards Organization
IT	-	Information Technology
MCA	-	Municipals, Counties and Agencies
MoICT	-	Ministry of Information and Communication Technology
NIST	-	National Institute of Standards and Technology
OISP	-	Organization information security Preparedness
PDCA	-	Plan-Do-Check-Act
TOE	-	Technology- Organization-Environment

CONCEPTUAL AND OPERATIONAL DEFINITION OF TERMS

ICT : Information and communication technology (ICT) is an extended term for information technology (IT) which stresses the role of unified communications and the integration of telecommunications, computers, enterprise software, middleware, storage, and audio-visual systems, which enable users to access, store, transmit, and manipulate information (Thaker, 2017). In this study ICT is used to refer to telecommunication facilities that enable people to access, store, transmit, and manipulate information.

E- Governance: It is the use of ICTs by government organizations for exchange of information with citizens, businesses or other government departments, faster and more efficient delivery of public services, improving internal efficiency, reducing costs and improving quality of services (N. Bindu, 2019).

Information Security: Preservation of confidentiality, integrity and availability of information (ISO/IEC 27000, 2016).

Information-Security Assessment: In this study information security assessment refers to a methodology for testing and measuring the current state of information security control measures so as to establish its ability to protect information against unauthorized access.

Information-Security Measures: These are technical or administrative safeguards and counter measures employed to avoid, counteract or minimize loss or unavailability of information due to threats acting on their corresponding vulnerability.

Risks: It is the possibility of harm or loss to any software, information, hardware, administrative, physical, communications, or personnel resource within an automated information system or activity (ISO/IEC 27000, 2016).

Information-Security Threats: Are events or activities, done deliberately or unintentionally, that have the potential for causing harm to an IT system or process (ISO/IEC 27000, 2016).

OISP: Organization Information Security Preparedness (OISP) is the percentage level of readiness an organization is at, regarding protection of its information systems.

County Government: Public administration of a county

E-governance Implementation: Setting up ICT facilities for public service delivery

CHAPTER ONE

INTRODUCTION

1.1 Overview

This chapter explored the background of the study and other concepts that were addressed in the research. Furthermore, it described the statement of the research problem, the research objectives, the research questions, and significance of the study, scope of the study, limitations and assumptions of the study.

1.2 Background to the Study

In an age where globalization and emerging technologies have taken root in every aspect of life, governments are now obligated to use new emerging and disruptive technologies to deliver public services. Governments are continually relying on information systems for efficient, accountable and transparent public service delivery (Nadu, 2013). E-governance is becoming a formal way of providing improved public services. E-governance is the application of ICTs to transform the efficiency, effectiveness, transparency and accountability of informational and transactional exchanges in government and to empower citizens through access and use of information (Bhattacharya, 2011). The resultant benefits of e-governance are less corruption, increased transparency, greater convenience, revenue growth, and cost reductions (Wamoto, 2015).

Countries globally are increasingly taking up on utilization of ICTs to deliver public services, increase transparency and engage people in decision-making processes. According to the United Nations E-Government Survey 2016, there has been an inclined rise in the number of countries utilizing advanced electronic and mobile services to provide public services online through one-stop platforms. More countries are making an

effort through electronic governance to ensure that public services are more accessible, effective, transparent and accountable. While developed countries, especially European countries and the United States of America, are leading in the use of ICTs to deliver public services, other developing countries - especially lower and middle income countries - are making good progress in adopting e-governance tactics to serve their citizens (UN Department of Economic and Social Affairs, 2016).

In Kenya, electronic governance has been supported momentarily as an ideal remedy for improving governance and enabling other critical functions of the government (Ochara, 2010). In 2004, the Kenyan government approved the e-government plan making the start of e-governance journey in Kenya (Wamoto, 2015). Since then, the government of Kenya initiated several e-governance systems with the aim of enhancing efficiency, transparency and democracy within public administration. Among these initiatives are the integrated financial management information system (IFMIS), integrated personnel and payroll database (IPPD), the local authorities integrated financial operations management systems (LAIFOMS), education management information system (EMIS), integrated taxation management systems (ITMS) currently known as ITAX, national integrated management information system (NIMIS), resource management system (RMS), health management information systems (HMIS), online recruitment and selection system for the public service commission and the border control system in the ministry of state for immigration and registration of persons (Ochara, 2010). Implementation of such systems have eased the burden of many citizens and improved government operation.

The implementation of these systems in developing countries like Kenya however, have encountered several challenges, which include technical challenges –like security and

privacy of information, inadequate infrastructure, financial challenges due to inadequate funding, social issues and human challenges (Meiyanti et al., 2019). Security and privacy of information is a major technical challenge facing e-governance initiatives in Kenya (Wamoto, 2015). Citizens' concerns about their information and transactions privacy is one of the major factors influencing the success of e-government initiatives.

Information security is a critical element in the implementation of any e-governance initiative (Shareef, 2016). Information security ensures that the confidentiality, integrity and availability of information are protected. In Kenya, various cases of information security breaches that have led to mistrust of e-governance initiatives have been recorded previously. According to the Kenya cyber security report 2016, the government faced many security breaches leading to financial loss and defamation of names. For instance, in 2015 the Garissa County government, reported that passwords of senior county staff were stolen and used to make illegal payments. Also the Ministry of Planning and Devolution IFMIS system was compromised by an inside attacker who stole login credentials of a government official who was in charge of approving tenders. The stolen credentials were used to approve fraudulent tender requests (Kenya Cyber security Report, 2016). In May 2017, a ransomware attack hit the country affecting most of the users running Windows operating systems. Phishing attacks targeting government's services and social media users were reported in 1st December 2014, where cyber criminals created fake websites and used them to collect login credentials, there after using the collected user's login details to advance their attacks (Business Daily, 2014).

Governments have accumulated a great deal of confidential information about their citizens, employees, customers, products, research, and financial status. Most of this information is collected, processed and stored electronically and transmitted across

networks to other computers. Reports show that the security of e-governance systems in Kenya's governments is at a high risk and information security threats against e-governance systems could cost the government millions of money ((Kenya Cyber security Report, 2016); (Serianu Cyber Threat Intelligence, 2016); (Cisco, 2017)).

In Kenya, information security in e-governance have been addressed using different approaches but still appear to be weak. For instance, the government of Kenya was reported to have lost over \$171million to cyber-criminal by the end of 2017, which is said to be the highest record in East Africa (Cisco, 2017). Today's governments and organizations employ very sophisticated security tools and technologies like firewalls, encryption, access control management, and others to curb this challenge. While advanced security technologies are fundamental parts of operational information security practices, it is disputed that appropriate security technologies alone are not adequate in addressing information security challenges (Otero, 2014).

In order to enhance information security, governments and organizations need to evaluate their information security practices on a regular basis so as to determine their security capability and thus review and update their information security practices to satisfy their specific security requirements and to overcome the challenge of the dynamic nature of information security threats (Otero, 2014).

The startling realities related to e-governance success in Kenya show existing insufficiencies and inadequacies in regards to information security practices employed to secure e-governance systems. These realities also serve as reasons for finding new ways to support governments and other organizations in improving their strategies for safeguarding their valuable information and systems. Therefore, it is vital that

information security practices and techniques around e-governance systems be evaluated and updated on regular basis.

Enhancing information security in e-governance not only nurture secure e-governance services, but also, builds confidence and trust in e-governance system users(Masau et al., 2011); leading to the success of e-governance initiatives (Karokola, 2012).

1.3 Statement of the Problem

According to Cisco cyber security annual report 2017, in East Africa Kenya recorded the highest loss of \$171 million to cyber criminals by the end of 2017. The public sector was ranked as the sector facing the highest information and cyber security risks in Kenya. This is so, not because the government has not invested in ensuring information security, but because of lack of realistic and prioritized strategies for improving organizational information security measures (Cisco, 2017). Due to the dynamic nature of information threats and emerging technologies, government should invest in techniques for regular assessment of information security strategies in order to establish the ability of the existing strategies in protecting information. This fact, therefore, necessitates the need for developing more efficient and innovative ways of evaluating organization's information security control measures. Departments responsible for critical government infrastructure need to have a consistent and interactive ways of identifying, assessing and managing organization's information security. Adequate evaluation of information security measures employed in governments is crucial in sustaining sound security as well as protecting information assets. Present information security assessment methodologies like risk assessment and management, best practice frameworks and other ad hoc approaches need to be reinforced and improved to assist governments with the process of information security management. In response to this, this study sought to

develop a web-based model for determining organization information security preparedness level in e-governance for county governments in Kenya. A web based model developed in this study is beneficial because of its ability to be accessed from anywhere and can be used across multiple device types. Furthermore, web-based systems allows centralized security reducing situations where sensitive corporate information are held on many local client PCs, which may not be secure and also eliminate the need for powerful client PCs.

1.4 Purpose of the Study

1.4.1 General Objectives of the Study

The main objective of the study was to develop a model for determining organization information security preparedness level in e-governance in Kenya's county governments.

1.4.2 Specific Objectives of the Study

The study was guided by the following specific objectives;

- i. To determine fundamental information security control measures that can be used in assessment of organization information security preparedness level
- ii. To develop a web based model for determining organization information security preparedness level in e-governance in Kenya's county governments
- iii. To implement the model for assessing organization information security preparedness in e-governance
- iv. To evaluate the effectiveness of the model in determining organization information security preparedness level in Kenya's County government.

1.5 Research Questions

The research sought to give answers to the following questions: -

- i. What are the fundamental information security controls that can be used to assess organization information security preparedness level in e-governance?
- ii. How can the model for determining organization information security preparedness level in e-governance be developed?
- iii. How can the model for determining organization information security preparedness level in e-governance be implemented?
- iv. How can the effectiveness of the proposed model for determining organizational information security preparedness level be evaluated?

1.6 Significance of the Study

As Kenya's remarkable ICT growth continues, ensuring the confidentiality, integrity, availability and assurance of e-governance services across Kenya's ICT infrastructure is of significant importance. Determining information security preparedness level is essential in ensuring that government critical e-governance infrastructure and systems are adequately protected. The main benefit of this study is that it provides a model in which the Kenya's county governments can use to evaluate organization information security preparedness level.

A successful model will enable county governments in Kenya to be proactive in defending their e-governance initiatives by knowing their level of information security preparedness level at any time. The findings of this study offer an insight guide to information security specialist in governments and other organizations on the fundamental information security control measures that can be used in assessment of organization information security preparedness level. Such a study provides a significant

addition to the body of knowledge in the area of e-governance security in Kenya's county governments. Further, this research opens up further strategic studies on e-governance security, organization information security and evaluation of information security, to students and other researchers who wish to conduct studies on these areas.

1.7 Justification of the study

An increase in information security threats is causing organizations and governments to take broader approach to assess their information security preparedness so as to ensure maximum protection of their critical information assets and systems. Lack of awareness of individual information security competency and capability levels makes it difficult for county governments to take proactive measures such as training for enhancement of information system security and improvement of information security practices in organization (Otero, 2014). Since governments are continuing to be the major targets for cyber criminals and the dynamic nature of information security threats, new and innovative ways must be created to solve every problem that affect the security of e-governance (Karokola, 2012). A web-based model proposed in this study, not only addresses the problem above, but also provides an effective and efficient way of assessing information security capabilities of key personnel in different departments dealing with e-governance security in governments.

1.8 Scope of the Study

The study focused on developing a model for determining information security preparedness level in e-governance in one of the county government in Kenya. The scope of deploying and implementing the model was also limited to one county. The data collected for providing the information required to develop the model were drawn from Uasin Gishu County. The study used Uasin Gishu county government as a representative

of the 47 county governments in Kenya. Uasin Gishu County is one of the 47 counties of Kenya, located in the former Rift Valley Province. Uasin Gishu County relies mainly on ICTs and electronic government to deliver public services. Furthermore, Uasin Gishu County is one of the county in Kenya that has automated most of its functions. Services like revenue collection, human resource management, and healthcare and staff recruitment have all been automated in Uasin Gishu County. In line with the Kenya's ICT Master Plan, Uasin Gishu county government like other county governments have adopted the use of ICT to deliver public services. For this reason, Uasin Gishu County was selected to undertake this study.

1.9 Limitation and Delimitations of the Study

The main constraint of this study was its scope and design. The scope of study was limited to Uasin Gishu County. Therefore, the findings may not necessarily be generalizable to other counties in the country due to circumstantial factors such as the demographic features and the levels of ICT adoption in delivering public services. Moreover, the study findings may not also automatically represent the situation in other county governments in the country. This can possibly affect the truthfulness of the results and the scope interpretation. This was however diminished by appropriate sampling to make it more representative of the information security situations in other counties.

The other limitation that could affect this study was the choice of instrument for data collection, the structured questionnaire preferred by this study is useful in surveys but lacks depth, and may have other limitations like researcher bias. Nevertheless, this constraint was mitigated by pre-testing the instrument before administration.

Ethical contemplations could hold back respondents from giving honest answers due to the fear of victimization and some respondents were not available to honor appointments during the study. Nonetheless, every effort was made to assure the respondents of their confidentiality and the academic nature of this study.

1.10 Assumptions of the Study

The researcher presumed that county government employees approached for this study appreciated the challenges associated with information security in e-governance implementation and the need for a solution to enable them to regularly assess the information security preparedness.

The researcher also made an assumption that the data collected from Uasin ishu County government provided a valid representation of sentiments shared by other counties in Kenya. However, this study can be further examined in other counties, government institutions and organizations to ascertain the correctness of the findings and therefore extend the applicability of this study to other organizations and government institutions.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

This chapter analyzed the available literature related to the study's main concepts and literature related to the objectives of the study in order to reveal what had been done and the research gap. It proceeded further to give the theoretical framework and the conceptual framework.

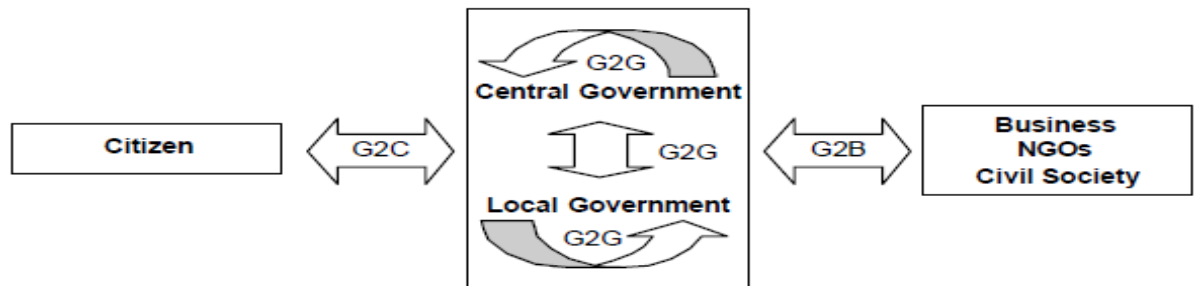
2.1.1 E-governance

In the last two decades, e-governance has gained more popularity in the world. Many management scholars have described the concept of e-governance as a means of reducing costs, improving services, saving time and increasing effectiveness and efficiency in the public sector(S. Singh & Karaulia, 2014). It is established that e-governance is the application of information and communication technologies to transform the efficiency, effectiveness, transparency and accountability of informational and transactional exchanges in governments and to empower citizens through access and use of information (N. Bindu, 2019). According to international organization, UNESCO, since governance refers to the exercise of political, economic and administrative authority in the management of a nation's affairs, including citizens' articulation of their interests and exercise of their legal rights and obligations, therefore, e-governance is described the performance of this governance via the electronic medium in order to facilitate an efficient, speedy and transparent process of disseminating information to the public, and other agencies, and for performing government administrative activities. Through e-governance, government services are made available to citizens in a convenient, efficient and transparent manner(Mohammed Alshehri & Drew, 2011).

There are three main target groups that can be distinguished in governance concepts. They are governments, citizens and businesses/interest groups (Salam, 2013).

Figure 1

Interaction between the Main Groups in E-governance



Source: Salam, (2013)

In e-governance, there are three basic delivery models available; government to-citizen (G2C) (customer), government-to-government (G2G) and government-to-business (G2B) (Bhattacharya, 2011) (Salam, 2013). Government to Citizen (G2C) relationship is the most basic aspect of e-governance. In modern times, government deals with many aspects of the life of a citizen. The relation of a citizen with the government starts with his/her birth and ends with his/her death. A person interacts with the government in every sphere of his/her life. The G2C relation includes the services provided by the government to the citizens. These services include the public utility services like telecommunication, transportation, medical facilities, electricity, education and also some of the democratic services relating to the citizenship such as certification, registration, licensing, taxation, passports, identification cards, among others. Therefore, e-governance in G2C relationship involves facilitation of the services flowing from government towards citizens with the use of information and communications technology. Government to government (G2G) relationship includes the relationships between county and state government and also the relationship between two or more

government departments. It includes the implementation of ICT in the functioning of the government, internally and externally. Government-to-Business (G2B) is an online non-commercial interaction between local and central government and the commercial business sector with the purpose of providing businesses information and advice on business best practices.

Despite the setbacks accompanied with e-governance, e-governance has brought about remarkable benefits to the government(M Alshehri & Drew, 2010). It is essential that information systems used to deliver e-governance services are managed in an ethical and accountable manner throughout to ensure that information is accurate, relevant, timely, available and secure. Enhancing information security in e-governance will nurture safe e-governance services and in return build user confidence and trust in e-governance systems; resulting to the success of e-governance initiatives(Karokola, 2012)

2.1.2 A Review of E-Governance in Kenya

Governments are obliged to provide essential services to its citizens. Since evolution of state and governments in 1970's, the delivery of public service have developed with advancement of technology. In the current information age, service delivery has been transformed in a greater way than in any other age due to the advancement of technology(S. Singh & Karaulia, 2014). It has been documented that in the decade of nineties, there was major global shifts towards increased deployment of IT by governments due to emergence of the World Wide Web(N. Bindu, 2019). The technology as well as e-governance has come a long way since then. With the increase in internet and mobile connections, citizens are learning to utilize their new mode of access in various ways (Salam, 2013). Furthermore, citizens have started expecting more and more electronically enabled services from governments and corporate organizations to

advance their public, professional and personal lives. The government of Kenya is now obligated to provide wide access of information through the available technologies.

The Kenya's government launched the e-government plan in 2004, marking the start of e-government journey (Wamoto, 2015). The government has since initiated several e-government systems with the aim of enhancing efficiency, transparency and democracy within public administration. The Kenya's information communication technology landscape is mainly governed by the ministry of information, communications and technology through the ICT authority, the national communication secretariat (NCS), and communications authority of Kenya (Ministry of ICT, 2018). The ICT Authority manages the development and use of ICT in all government ministries and agencies while the communications authority of Kenya is the regulatory body for the communications sector in Kenya. The role of the NCS is to research and advice government on ICT policies(CIPESA, 2015).

In 2013, the government of Kenya commissioned an ICT master plan to guide implementation of information and communication technologies in support of achieving the vision 2030 goals(Government of Kenya, 2014). This Master Plan has three foundations and three pillars. The first pillar of the ICT Master Plan is e-government services, which aims at ensuring provision of e-government information and services as key to improving productivity, efficiency, effectiveness and governance in all key sectors. The second pillar is ICT as a driver of industry, which aims at transforming key Vision 2030 2nd medium term plan economic sectors to significantly enhance productivity, global competitiveness and growth; and the third pillar is developing ICT businesses that can produce and provide exportable quality products and services that are comparable to the best in the world. E-government ensure provision of e-government

information and services which are key to improving productivity, efficiency, effectiveness and governance in all key sectors(Wamoto, 2015).

Kenya enacted another constitution in 2010, which established a system of devolved government with 47 lower level county governments(The Republic of Kenya, 2010). The operation of the county governments started in March 2013 after the elections, which included the election of county governors, deputy governors and representatives. With this devolvement, ICT infrastructure and services are fundamental to development in each county government.

The government through ICTA developed Government Enterprise Architecture (GEA) framework to guide each county government and other government ministries with the planning and implementation of ICTs in ensuring the realization of e-governance(ICT Authority, 2016a). The GEA framework establishes a set of policies and technical adoptions that work toward achieving desired results, technical standardization and integration in the public sector. The GEA framework recommends a method and describes the minimum components of an ICT Plan, and its following standards provide sufficient procedures on how to implement the ICT plan in government agencies. The GEA is a mission-focused framework for ministries, its department, and its constitutional bodies to improve government performance. By aligning governments, business processes, information flows, and technology consistently across and throughout the government, the GEA builds a blueprint for improving e-governance programs.

For developing an information security management system, the GEA provides an information security standard based on ISO/IEC 27001. This standard acts as a guideline to all governments agencies when developing an information security management system(ICT Authority, 2016b). The standard is based on a risk management approach

and requires ministries, counties and agencies to implement policies and procedures that are proportionate to their level of risk, after conducting and documenting a risk assessment.

2.1.3 Information Security

Information security means protecting information and information systems from unauthorized access, use, disruption, or destruction(Nieles & Dempsey, 2017). Information security is a key factor towards achieving organization overall security and business objectives. Information security involves protecting information that is in computer storage, processing, or transit in distributed networks. Information security's principal focus is the balanced protection of the confidentiality, integrity and availability of data while maintaining a focus on efficient policy implementation, all without obstructing organization productivity(A. Singh et al., 2014).

It is impossible to achieve ideal information security. This is because information security is a dynamic and never ending process that involves an ongoing training, assessment, protection, monitoring and detection, incident response, documentation, and review(A. Singh et al., 2014). Information security focuses on people, processes and technology(Krishna, 2010). When correctly assembled, the people, technology, and process elements of an information security work together to secure information systems and to achieve organizations' objectives. In today's organizations, information security is equated to an assurance that the information risk associated with the use of information technology are balanced with the control measures taken to protect them.

In e-governance, information security enables governments to meet their goals by implementing systems with due consideration of information technology related risks to the governments, organizations, business and trading partners, technology service

providers, and most importantly its citizens. According to National e-governance Plan 2010, governments meet information security goals through striving to accomplish the following objectives:

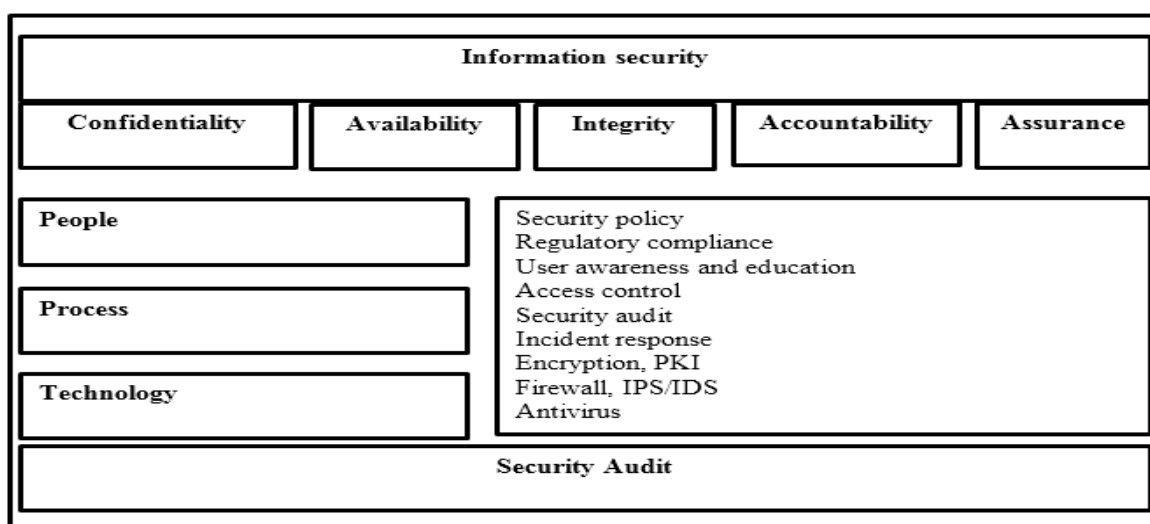
- i. Ensuring availability of e-governance services by enforcing procedures, policies, and controls used to ensure only authorized users have prompt access to information. This objective protects against intentional or accidental attempts to deny legitimate users access to information or systems.
- ii. Ensuring integrity of data and systems by enforcing procedures, policies, and controls used to ensure that information cannot be altered in an unauthorized manner and that systems are free from unauthorized manipulation that will compromise accuracy, completeness, and reliability.
- iii. Ensuring confidentiality of data and systems by enforcing procedures, policies, and controls employed that protect information of citizens, private businesses and governments against unauthorized access or use.
- iv. Ensuring accountability by enforcing procedures, policies, and controls necessary that trace actions to their source. Accountability directly supports non-repudiation, deterrence, intrusion prevention, security monitoring, recovery, and legal admissibility of records.
- v. Ensuring assurance: Assurance addresses the procedures, policies, and controls used to develop confidence that technical and operational security measures work as intended.

As illustrated in figure 2, information security works towards achieving confidentiality, integrity, availability, accountability and assurance of information. This is achieved when the three elements of information security (people, process and technology) work together effectively using various control measures that include access controls, security

policies, user awareness and education, antiviruses, firewall among others. Furthermore, to achieve ideal information security, security audit should be done regularly to assess the ability of installed control measures to ensure confidentiality, availability, integrity, accountability and assurance of information.

Figure 2

Information Security Model



Source: National e-Governance Plan, (2010)

Information security is an essential tool for managing information security risks and threats in any environment. Security spans through an entire organization starting from the strategic level to the tactical and operational levels) (Karokola, 2012).

Information security is achieved through the implementation of an applicable set of controls, selected through the chosen risk management process and managed using ISMS, including policies, processes, procedures, organizational structures, software and hardware to protect the identified information assets(ISO/IEC, 2016). These controls need to be specified, implemented, monitored, reviewed and improved where necessary, to ensure that the specific information security and business objectives of the

organization are met. The careful implementation of information security controls is paramount to protecting an organization's information assets as well as its reputation, legal position, personnel, and other tangible or intangible assets(Nieles & Dempsey, 2017).

2.1.4 Information Security Challenges Affecting E-Governance

The elevated risk that comes with the use of ICT in governance threatens the success of e-governance in achieving its objectives. E-governance offers governments with an enhanced way of improving public service delivery. Although there are different initiatives in place set out to address information security issues, governments are facing escalated security challenges in e-governance implementation(Edet & Abasilim, 2015). Some of the recurrent information security challenges affecting organizations available in existing literature include:

i. Disintegration of information security management programs

Ahmad & Mohammad (2012) described disintegrated governance, information security management (ISM) and compliance efforts as one of the challenges facing information security management. Governance consists of the leadership, organizational structures and processes that ensure that the organization's ICT sustains and extends the organization's strategies and objectives. Compliance encompasses external laws, regulations, obligations and internal policies that must be observed by an organization with respect to their corporate morality and risk tolerance. On the other hand, information security management is about policies and procedures for systematically managing an organization's sensitive data. Therefore, the inability of governance, information security management system and compliance efforts to integrate affects organization information security capability.

Patil (2008) concurred with Ahmad & Mohammad statement by stating that the cause of security breaches in organization is lack of a comprehensive information security measure that can bring together standalone security components. He argues that the problem with organizations information security programs is the disintegration of security management efforts employed by organization to address their security issues. The security components in software development, policies and procedures, incident management, business continuity management, regulations & audit are implemented separately as illustrated in the Figure 3.

Figure 3

Problem Space: Security Islands



Source: (Patil, 2008)

As demonstrated in figure 3, security islands caused by isolation of information security control measures implemented in different components of an electronic system undermines the holistic approach of information security management. Independence of these measures results in inconsistencies, security deserts, and isolated security processes, waste of resources and inefficient security measures (ICT Authority, 2016b).

ii. **End user non-compliance with Information Security Policies and Controls**

Hassan (2013) observed that the cause of security failure in organization is end-user non-compliance with information security policies and controls. This may not be intentional but largely because of ignorance. The managerial style in an organization has a significant influence on the employee behavior in the organization. Absence of senior management commitment and support contribute to the failure of information security management plans(Ahmad & Mohammad, 2012). The senior management in any organization is responsible for influencing the adoption of a security culture, allocating budgets on IT security investment, information security awareness training and creation of policies to guide information security management. Failure of the senior management to support information security management results in lack of policies to guide information security management, poor and misplaced budgets on IT security, lack of information security awareness program in the organization and non-compliance to security policies(Hassan, 2013).

iii. **Inappropriate Security Practices**

Inappropriate information security practices give organizations/governments a false sense of security. With the evolving nature of information security threat, information security practices that may have been efficient a year ago can rapidly diminish and become limiting today. Routine assessment of information security practices help organizations and governments stay proactive. With the right information, security practices organizations and governments can quickly adapt to the present changes.

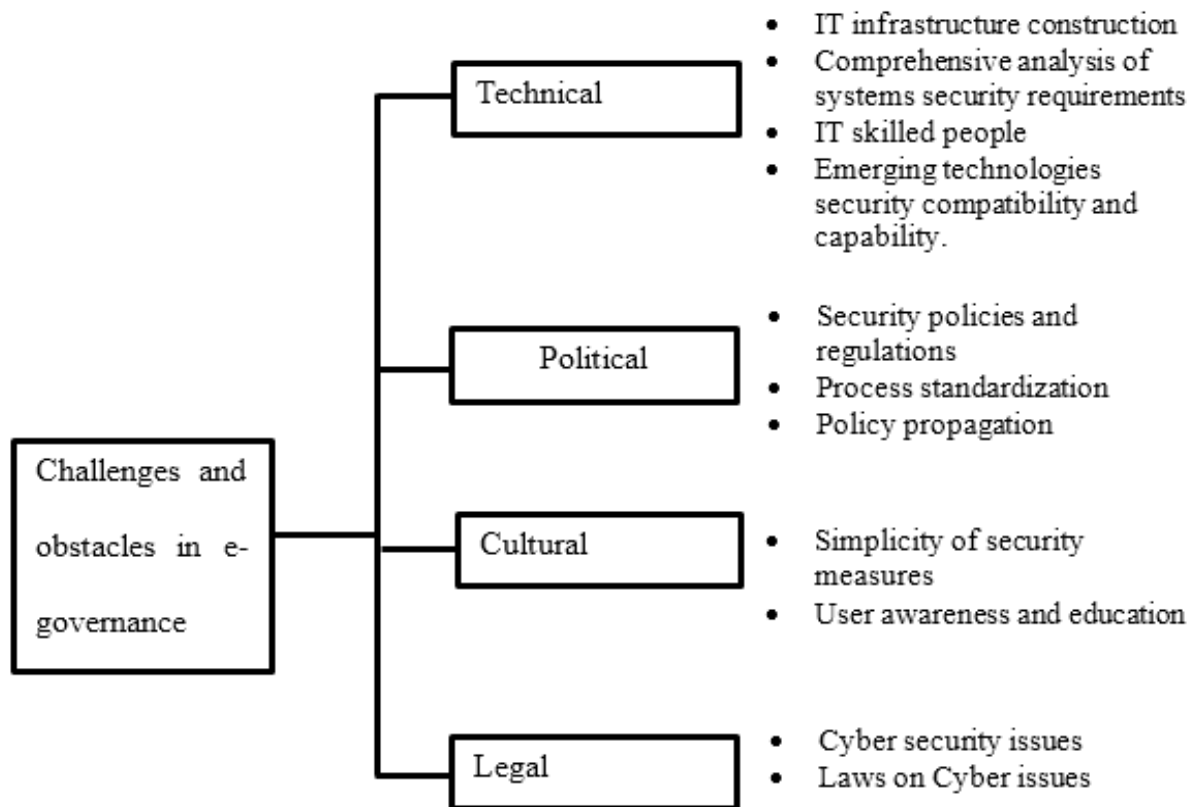
iv. **Technical and Non-Technical Threats**

According to Shareef (2016), information security challenges facing organizations and governments can be viewed in two main categories, technical and non-technical

challenges. Non-technical challenges can be further categorized into three other perspectives; political, cultural and legal aspects. These aspects if properly incorporated in a security practices will yield to better information security management in e-governance. The figure 4 below illustrates these challenges.

Figure 4

Challenges in E Governance



Source: Shareef, (2016)

According to Karokola (2012), the technical aspects of information security comprise vulnerabilities caused by faulty system design, development, implementation, configuration, integration, and maintenance. Furthermore, he claims that non-technical aspects of information security result from lack of administrative and managerial policies, moral and cultural norms, legal and contractual documents, operational and

procedural guidelines and awareness programs that strengthen organization information security.

2.2 Information Security Control Measures

Information security controls are technical or administrative safeguards and counter measures employed to avoid, counteract or minimize loss or unavailability of information due to threats acting on their corresponding vulnerability(Keung, 2014). Information security controls seek to protect the confidentiality, integrity, availability and assurance of information.

National institute of Standards and Technology (NIST) lists the three primary categories of controls as administrative, technical and physical (Keung, 2014). Administrative controls are primarily, procedures and policies, which are created to define and guide employee actions in dealing with the organizations' sensitive information. Technical security controls consist of those hardware and software features provided in a system that helps to ensure the integrity and security of data, programs and operating systems. Physical security controls are means and devices employed to control physical access to sensitive information and to protect the availability of the information(Eduardo & Junior, 2015).

Security controls can be further classified based on the phase of activities involved in implementing them and the purposes for which they are implemented(Northcutt, 2019).

Information security controls can be grouped as preventive controls, detective controls, or corrective controls depending on the objective of implementation. Preventive controls are implemented to prevent the threat from coming in contact with the weakness. Detective controls are controls that identify that the threat has landed in systems.

Corrective controls are controls that mitigate or lessen the effects of the threat being manifested.

Table 1

Information Security Controls

Preventive	Detective	Corrective
Security awareness training	System monitoring	OS Upgrade
Firewall	IDS	Backup data restoral
Anti-virus	Anti-virus	Anti-Virus
Security guard	Motion detector	Vulnerability mitigation
IPS	IPS	

Source: Northcutt, (2019)

Information security control measures are core components of organization information security management system. They are administered to prevent, detect and correct information security risk through administrative, technical and physical means.

ISO/IEC 27001 employed by the Government Enterprise Architecture to manage information security for Kenya’s ministries, counties and agencies specifies 114 information security controls in 14 groups (ICTA standards, 2016). The information security controls groups highlighted by the standard are; Information security policies, Organization of information security, Human resources security - controls that are applied before, during, or after employment, Asset management, Access controls, Cryptography, Physical and environmental security, Operational security, Communications security, System acquisition, development and maintenance, Security for suppliers and third parties, Incident management, Business continuity/disaster recovery (to the extent that it affects information security), Compliance - with internal requirements, such as policies, and with external requirements, such as laws.

Information security policies are guidelines put in place to provide an organization with direction and support for information security in accordance with business objectives and applicable laws and regulations. This group of control contains a set of two information security control objectives; information security policies and review for information security policies(ISO/IEC 27001, 2013).

Organization of information security contains seven control objectives that provide guidelines for internal organization of information security and mobile devices and teleworking. The objectives of these controls are; to establish an organization structure to initiate and control the implementation and operation of information security within the organization, and to safeguard the security of teleworking and use of mobile devices.

Human resource security contain six controls that are applied before, during and after employment. Prior to employment these controls ensure that employees and suppliers realize their duties and they are suitable for the roles for which they are considered. During employment, the controls ensure that employees and suppliers are cognizant of their information security responsibilities. After employment, controls ensure that the organization's interests are protected as part of the practice of shifting or ending engagement.

Asset management contain ten control objectives that provide guidelines on who is responsible for the various assets of an organization, classification of information and handling of media devices. The objectives of these controls are; to identify organizational assets and define appropriate protection responsibilities, to ensure that information receives an appropriate level of protection in accordance with its importance to the organization, and to prevent unauthorized disclosure, modification, removal or destruction of information stored on media(ISO/IEC 27001, 2013).

Access controls contains fourteen controls that outline business requirements of access control, management of users, responsibilities of users, and system and application access controls. The objectives of these controls are to; ensure approved user access and to deter illegal access to systems and services, make users responsible for safeguarding their validation information, and prevent unapproved access to systems and applications.

Cryptography contain two cryptographic controls that ensure correct and effective use of cryptography to safeguard the confidentiality, authenticity and integrity of information.

Physical and environmental security contain fifteen control objectives that outline controls on secure areas and equipment security. The objectives of these controls are to; prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities, and to prevent loss, damage, theft or compromise of organization resources and disruption of the organization's processes.

Operations security has fourteen controls that specify procedures and responsibilities of operations, protection of malware, backup, and logging and monitoring. Furthermore, it contains controls that ensures control of operational software, technical vulnerability management and information audit concerns. The aim of this group of controls is to;ensure correct and secure operations of information processing facilities, protect information and information processing facilities against malware, provide information backup, and record events and generate evidence. Additionally, they ensure the integrity of operational systems, and prevent exploitation of technical vulnerabilities and minimize the impact of audit activities on operational systems(ISO/IEC 27001, 2013).

Communications security has seven controls that outlines controls on network security management and information transfer. These controls ensure that information in

networks and its subsidiary information processing facilities are protected and that the security of information transmitted within and outside the organization is maintained.

System acquisition, development and maintenance contain thirteen controls that specify security requirements of information systems, security in development and maintenance of systems, and protection of data used in testing of systems. The objective is to ensure that information security is designed and implemented within the development lifecycle of information systems.

Supplier relationships contains five controls on security for suppliers and third parties. They state controls on supplier service delivery management and information security in supplier relationships. The objectives are to ensure protection of the organization assets that are available to suppliers and to uphold an agreed level of information security and service delivery in line with supplier agreements(ISO/IEC 27001, 2013).

Incident management contains seven controls that describe the management of information security incidents and enhancements. The objective of these controls is to ensure a consistent and effective approach to the management of information security incidents, including communication on security proceedings and vulnerabilities.

Business continuity/disaster recovery contains four controls that describe aspects of information security in business continuity and availability of information processing systems all times. The objective of these sets of controls is to ensure that information security continuity is included in the organization's business continuity management systems.

Compliance is the last group of controls that is outlined in the ISO/IEC 27001 standard. It has eight controls that cover compliance with legal and contractual requirements and information security reviews. The aim of this group of controls is to prevent

incompliance to legal, statutory, regulatory or contractual obligations related to information security. Furthermore, it ensures that that information security is realized and operated in accordance with the organizational guidelines and procedures(ISO/IEC 27001, 2013).

2.3 Information Security Roles and Responsibilities

In order for organizations, regardless of size, to achieve the information security objectives, it is important for them to clearly define the roles and responsibilities of their professionals. Professionals who take responsibility for protecting networks, infrastructure, and computer systems are IT security professionals(Nieles & Dempsey, 2017). These roles include system administrators, network security officers, information security engineers, application security engineers, network managers, network engineers, chief information officer (CIO), chief technology officer (CTO), chief security officer (CSO), chief information security officer (CISO), information assurance manager (IAM), and computer operators.

Information security professionals are tasked with protecting information systems and providing access to information for users based on their necessity and identity. In this study it is important to identify key information security personnel present in an organization and their key responsibilities in enforcing information security.

2.4 Information Security Assessment

Information security assessment is the process of determining how effectively an entity being assessed (such as host, system, network, procedure, and person) meets specific security objectives (Scarfone & Orebaugh, 2008). Information security assessment practices vary between industries, disciplines, and even within the same organization, which has brought about many different approaches of assessing information security in

an organization. There are three broad categories of assessment methods that can be used to assess information security measures; testing, examination, and interviewing. Testing is the process of analyzing one or more assessment objects under specified conditions to compare actual and expected behaviors. Examination is the process of checking, inspecting, reviewing, observing, studying, or analyzing one or more assessment objects to facilitate understanding, achieve clarification, or obtain evidence. Interviewing is the process of conducting discussions with individuals or groups within an organization to facilitate understanding, achieve clarification, or identify the location of evidence. Assessment results are used to support the determination of security control effectiveness over time.

There are different existing methodologies for information security assessment developed by different organizations and researchers to assist organizations assess their information security preparedness.

2.4.1 Baldrige Cyber Security Excellence Builder (BCEB)

The Baldrige Cyber security Excellence Builder is a self-assessment method that help organizations examine and understand the effectiveness of their cyber security risk management efforts and identify improvement opportunities in the context of their overall organizational performance (NIST, 2019). This self-assessment method merges organizational assessment approaches from the Baldrige Performance Excellence Program (BPEP) with the concepts and principles of the Cyber Security Framework developed by NIST's Applied Cyber Security Division (ACD). The BCEB merges the organizational performance and systems perspectives of the Baldrige Excellence Framework with the holistic, enterprise-based approach of the Cyber security Framework.

Figure 5

Baldrige Cybersecurity Excellence Builder Components



Source: NIST, (2019)

The Cyber security Framework gathers and categorizes standards, guidelines, and practices that are working effectively in other organizations. The BCEB is intended for use by the leaders and managers in an organization who are concerned with and responsible for mission-driven, cyber security-related policy and operations.

2.4.2 NIST Framework for Cyber Security Risk Assessing

This method was developed by the National Institute of Standards and Technology to assess cyber security risks during the implementation of NIST cyber security framework. The method forms a section of the NIST Cyber Security Framework that allows organizations to measure and assign values to their risks along with the cost and benefits of steps taken to reduce risks to an acceptable level(National Institute of Standards and Technology, 2018). This self-assessment method is designed to help organizations implementing the NIST Cyber Security Framework to improve their decision making process about investment priorities. The NIST assessment method measures an organization's cyber security posture in relation to the CSF(Barrett, 2018).

In addition, the National Institute of Standards and Technology provides a guide to the basic technical aspects of conducting information security assessments (Scarfone & Orebaugh, 2008). The guide presents technical testing and examination methods and techniques that an organization can use as part of their assessment, and offers insights to assessors on their execution and the potential impact they may have on systems and networks. For an assessment to be successful and have a positive impact on the security posture of a system, elements beyond the execution of testing and examination must support the technical process. Suggestions for these activities, including a robust planning process, root cause analysis, and tailored reporting, are also presented in the guide. The assessments focus on verifying that a particular security control meets requirements, at the same time identifying, validating, and assessing a system's exploitable security weaknesses. This guide is not intended to present a comprehensive information security testing or assessment program, but rather an overview of the key elements of technical security testing and assessment with emphasis on specific techniques, their benefits and limitations, and recommendations for their use.

2.4.3 Maryland Health Care Commission Cyber Security Assessment Method

This Cyber security assessment method was developed by the Maryland Health Care Commission to assist small health care providers in identifying gaps and potential risks in their cyber security processes (Maryland Health Care Commission, 2019). The method is also used to provide guidance in the development and implementation of cyber protections where cyber security processes do not exist. The method was developed using the NIST Cyber security Framework, which assembles standards, guidelines, and practices to evaluate cyber security. The method guides users through assessing the organizational processes that address the five core functions of the NIST cyber security framework: identify, protect, detect, respond, and recover. The scope of this assessment

method is within Maryland Healthcare in the United States of America and can only be adopted by other health institutions using the NIST cyber security framework. Its applicability is limited and cannot be scaled to other organizations.

2.4.4 FIFIEC Cyber Security Assessment Method

In light of the increasing volume and sophistication of cyber threats, the Federal Financial Institutions Examination Council (FFIEC) developed the cyber security assessment method on behalf of its members, to help institutions identify their risks and determine their cyber security maturity (Federal Financial Institutions Examination Council, 2017). The method uses a list of questions to identify the level of risk and to assess the status of the existing cyber security programs. The aspects of the assessment are consistent with the principles of the FFIEC Information Technology Examination Handbook and the NIST Cyber security Framework, as well as industry accepted cyber security practices. The assessment provides institutions with a repeatable and measureable process to inform management of their institution's risks and cyber security preparedness. The assessment consists of two parts: inherent risk profile and cyber security maturity. The inherent risk profile identifies the institution's inherent risk before implementing controls. The cyber security maturity includes domains, assessment factors, components, and individual declarative statements across five maturity levels to identify specific controls and practices that are in place. While management can determine the institution's maturity level in each domain, the assessment is not designed to identify an overall cyber security maturity level. The scope of this method is that it's a risk assessment method and is limited to FFIEC information technology examination handbook and the NIST cyber security framework.

2.4.5 Information Security Risk Assessment

Information security risk assessment is a systematic approach used to identify organizations needs regarding information security requirement (ISO/IEC 27000). It is used by information security best practices as part of information security risk management process which focuses on identifying the relevant risks and the appropriate controls for reducing or eliminating these identified risks. Risk assessment quantifies or qualitatively describes the information security risk and enables organizations to prioritize risks according to their seriousness. It determines the value of an information assets, identifies the applicable threats and vulnerabilities that exist, identifies the existing controls and their effect on the risks identified, determines the potential consequences and finally prioritizes them.

According to the ISO/IEC 27000 standard, common information security risk assessment methodologies involves nine primary steps that help in conducting an information risk assessment; system understanding, threat identification, vulnerability identification, control analysis, likelihood determination, impact analysis, risk determination, control recommendation, and results documentation (ISO/IEC, 2016). First, an organization makes an inventory of information assets, procedures, processes and personnel to understand what the key information assets are and which pose the highest risk. Risks are generally calculated as the impact of an event multiplied by the frequency or probability of the event. This will therefore help in determining the risks and opportunities that need to be addressed.

2.4.6 Fuzzy Theory Model for Assessing Information Security Controls

Otero (2015) in his dissertation, *An Information Security Control Assessment Methodology for Organizations*, developed a method for evaluating information security

controls in organizations. The methodology was created using the fuzzy logic toolbox of MATLAB, which is based on fuzzy theory and fuzzy logic. This assessment model allows more accurate assessment of unknown measures (Otero, 2015). Moreover, the methodology considers all-inclusive scenarios when evaluating information security controls and prioritizes specific information security controls in line with an organizations business objective. Nevertheless, the method requires identification of associated functions of the fuzzy sets, definitions of semantic variables, and fuzzy operators in order to model the patterns and assumptions of an organization regarding the relevance of an information security control. Specifically, fuzzy sets must be indicated with regard to the objective function, constraints established, as well as terms and associative functions of the semantic variables.

2.4.7 Data Protection Assessment Method

Data protection assessment is a self-assessment method created by ICO (Information commissioner office), UK, to help organizations assess their compliance with data protection law(The Information commision office, 2019). It contains data protection assurance checklists that a controller or a processor uses to assess their compliance with common data protection laws that include information security, data sharing and privacy and records management. The information security section assesses an organizations compliance with data protection laws in the specific areas of information and cyber security policy and risk, mobile and home working, removable media, access controls and malware protection.

2.4.8 CS²SAT: The Control Systems Cyber Security Self-Assessment Tool

In 2007, the department of homeland security national cyber security division, United States of America, developed the Control System Cyber Security Self-Assessment Tool

(CS²SAT) that provides users with a systematic and repeatable approach for assessing programmatic aspects of the cyber-security position of industrial control system networks(Lee, 2008). The CS²SAT is a standalone application software that guides users through a systematic process to collect facility-specific control system component information and then make appropriate recommendations for improving the system's cyber-security posture. The CS²SAT provides recommendations from a database of industry available cyber-security practices, some of which have been adapted specifically for application to industrial control system networks. The purpose of the CS²SAT is to identify missing security controls and make recommendations rather than measure the security posture or risk level of an organization.

2.5 Existing Frameworks

There are plenty of standards, models and frameworks for information security management that are accepted internationally. These standards and frameworks provide a foundation and guidance for establishing a security culture in any organization and performing information security assessment. It also outlines information security indicators and targets that are used to assess the current state of information security in any organization. Existence of many security frameworks and standards gives organization the flexibility of choosing those frameworks that will satisfy their needs.

Some of the standards and frameworks considered as benchmarks for information security self-assessment are discussed in this study and are used as a foundation for designing and developing the proposed model for determining organizational information security preparedness in Kenya.

ISO/IEC 27001, COBIT5 and NIST have been used widely as foundational frameworks for creating a sound information security environment in big and small organizations.

These internationally acceptable frameworks and standards specifies requirements for planning and implementing an effective information security management system, ensuring that appropriate controls are nominated to protect organization's information (Roesnita Ismail, 2013). They also provide a series of controls that are required to ensure maximum protection of information assets. Most of the controls provided by these frameworks and standards overlap in categories of preventive, corrective and detective levels at the same time correspond to the groups of administrative, technical and physical security controls .

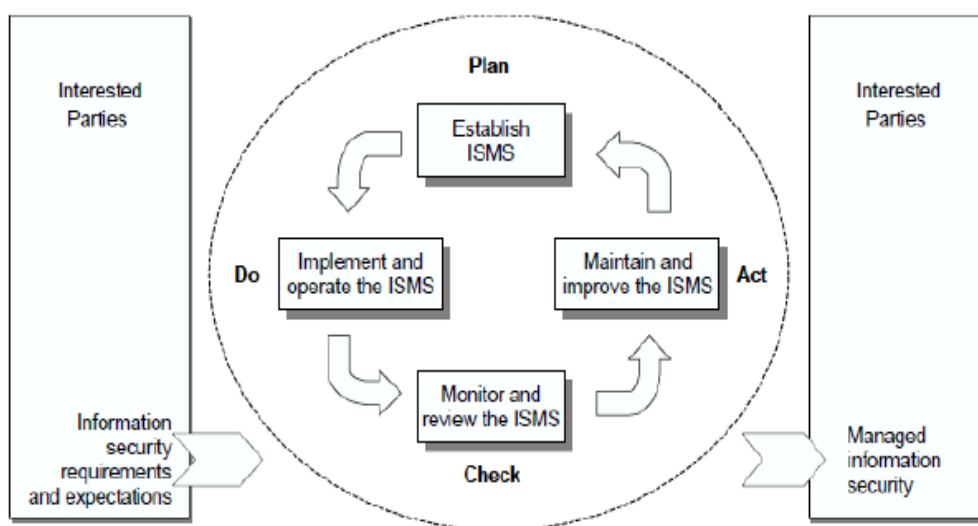
The next section provides a detailed overview of the frameworks that informed this study.

2.5.1 ISO/IEC 27001 Standard

The ISO/IEC 27001 standard was created jointly by the International Standards Organization and the International Electro-Technical Commission. This international standard specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving formalized information security management systems within the context of the organization's overall business risks (ISO/IEC 27000, 2016). It specifies requirements for the implementation of information security controls customized to the needs of individual organizations or parts thereof. It is designed to ensure the selection of adequate and proportionate security controls to protect information assets. It is seen as an internationally recognized structured methodology dedicated to information security management. The standard introduces the Plan-Do-Check-Act (PDCA) model that aims to establish, implement, monitor and improve the effectiveness of an organization's ISMS. The PDCA is an iterative, four-stage approach for recurrent improvement of information security in organizations.

Figure 6

PDCA Model



Source: ISO/IEC, (2005)

The plan phase of the PDCA model refers to establishment of an ISMS policy, objectives, processes and procedures relevant to handling risk and improving information security to deliver results in accordance with the organization's objectives and policies(ISO/IEC, 2005). Do refers to implementing and operationalizing the ISMS policy, controls, processes and procedures. Check refers to evaluating and, where relevant, measuring the process performance against ISMS policy, objectives and practical experience and report the outcomes for the organization to review. Act refers to taking corrective and preventive actions, based on the results of the in-house ISMS audit and organization review or other appropriate information, to achieve persistent perfection of the ISMS(Ristov et al., 2011).

The ISO/IEC 27001 document references valuable details on information security risk that can be used as selection criteria for a proper information security risk assessment approach that builds upon the controls list proposed by the standard. The controls are

grouped into fourteen control objectives; information security policies, organization of information security, human resource security, asset management, access control, cryptography, physical and environmental security, operation security, communication security, system acquisition development and maintenance, supplier relationship, information security incident management, information security aspects of business continuity management, and compliance. These controls work together to manage information risks as discussed in section 2.2 on information security controls.

2.5.2 National Institute of Standards and Technology (NIST) Cyber Security Framework

The NIST Cyber Security Framework is a USA cyber security voluntary framework that is based on NIST existing standards, guidelines, and practices for reducing cyber risks to critical infrastructure (National Institute of Standards and Technology, 2019). The Framework consists of standards, guidelines, and practices to promote the protection of critical infrastructure.

The NIST cyber security framework consist of three components; the core, the tier and the profile.

Figure 7

Components of NIST Cyber Security Framework



Source: National Institute of Standards and Technology, (2019)

The framework core is a set of cyber security activities, desired outcomes, and applicable references that are common across critical infrastructure sectors. The core presents industry standards, guidelines, and practices in a manner that allows for communication of cyber security activities and outcomes across the organization from the executive level to the operational level (Nieles & Dempsey, 2017). The framework core consists of five coexisting and continuous functions; identify, protect, detect, respond, recover. When considered together, these functions provide a high-level, strategic view of the lifecycle of an organization's management of cyber security risk. The framework core then identifies underlying key categories and subcategories for each function, and matches them with example informative references, such as existing standards, guidelines, and practices for each subcategory.

Figure 8

Core function of NIST Cyber Security Framework



Source: National Institute of Standards and Technology, (2019)

The framework implementation layers assist organizations by providing context on how an organization views cyber security risk management. The steps guide organizations to consider the appropriate level of precision for their cyber security program and are often used as a communication tool to discuss risk level, mission priority, and the budget.

Framework profiles are an organization's distinctive orientation of their organizational requirements and objectives, risk levels, and resources against the desired outcomes of the framework core. Profiles are mainly used to identify and prioritize opportunities for improving cyber security at an organization.

NIST framework specifies the 20 controls; access control, awareness and training, audit and accountability, security assessment and authorization, configuration management, contingency planning, identification and authentication, incident response, individual participation, privacy authorization, maintenance, media protection, physical and environmental protection, planning, personnel security, risk assessment, system and services acquisition, system and communications protection, system and information integrity, and program management(Nieles & Dempsey, 2017).

Access controls specifies requirements for granting or denying specific requests to systems or facilities. Examples of access control security controls include: account management, separation of duties, least privilege, session lock, information flow enforcement, and session termination. Awareness and training controls ensure that users are aware of their security responsibilities and are taught the correct practices to help the change their behavior towards information security. Audit and accountability controls describes techniques for reviewing and examining records and activities to assess the adequacy of system controls and ensure compliance with established policies and operational procedures. Audits assist in detecting security violations, performance issues, and flaws in applications. Media protection controls addresses the defense of system media whether digital and non-digital.

Physical and environmental security controls protect systems, buildings, and related facilities against threats associated with their physical environment. Personnel security tries to minimize the risk that employees and suppliers pose to organizational assets through the illegal use or exploitation of legitimate access to the organization's resources. Risk assessments identify and prioritize risks to organizational operations, assets, individuals, and related stakeholders that may result from the operation of a system. Examples of risk assessment controls include; security categorization, risk assessment, vulnerability scanning, and technical surveillance countermeasures survey. System and service acquisition controls emphasizes on the need of planning and managing information security managed throughout a system's life cycle, from initial planning to design, implementation, operation, and disposal. Examples of system and service acquisition controls include; allocation of resources, acquisition process, system documentation, supply chain protection, trustworthiness, criticality analysis, developer-provided training, component authenticity, and developer screening. System and

communications protection controls provide an array of safeguards for the system through physical or logical means. System and information integrity controls provide assurance that the information being accessed has not been meddled with or damaged by a fault in the system. Program management controls entails the development of a comprehensive management approach that manages system security at multiple levels.

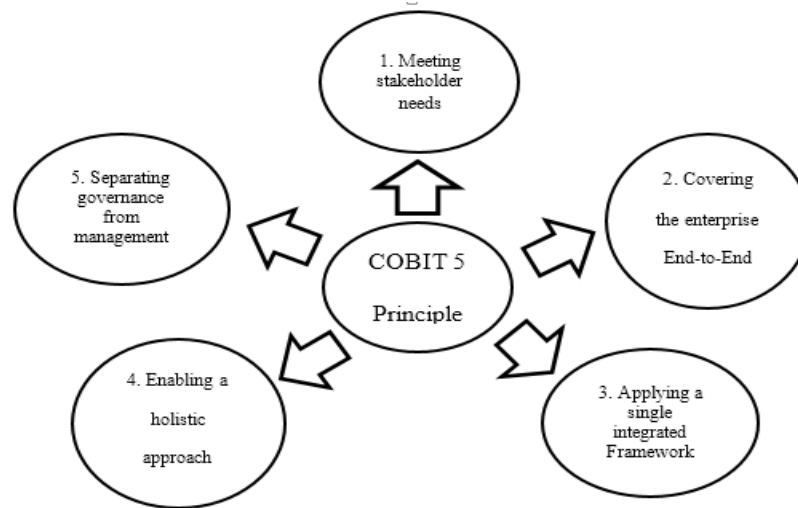
2.5.3 Control Objectives for Information and Related (COBIT 5) for Information Security

COBIT is a framework developed in the mid-90s by ISACA, an independent organization of IT governance professionals (ISACA, 2012). This framework started out primarily focused on reducing technical risks in organizations, but evolved to include alignment of IT with business-strategic goals. COBIT 5 for Information Security provides guidance to help IT and security professionals understand, utilize, implement and direct important information security-related activities, and make more informed decisions while maintaining awareness about emerging technologies and the accompanying threats. COBIT 5 enables information and related technology to be governed and managed in a holistic manner for the whole enterprise, taking in the full end-to-end business and functional areas of responsibility, considering the IT-related interest of internal and external stakeholder.

The COBIT 5 principles and enablers are generic and useful for enterprises of all sizes whether commercial or public sector.

Figure 9

COBIT 5 Principles

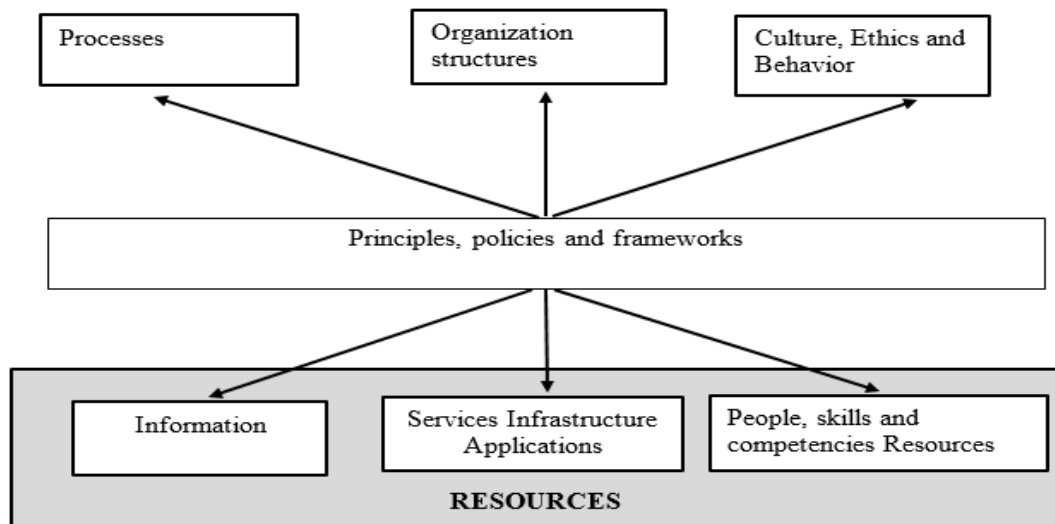


Source: ISACA, (2012)

COBIT 5 defines a set of enablers to support the implementation of a comprehensive governance and management system for enterprise IT.

Figure 10

COBIT 5 Enablers



Source: ISACA, (2012)

From Figure 10 above, there are seven enablers of COBIT 5 that influence the success of an initiative in an organization; principles, policies, and frameworks, processes, organizational structures, culture, ethics, and behavior, information, services, infrastructure, and applications, people, skills, and competencies.

The principles, policies, and frameworks are devices that are used to communicate the rules of the organization. The processes enabler provides a detailed reference guide to the processes defined in the process reference model which subdivides the IT-related practices and activities of an organization into two main areas; governance and management. Organizational structure gives a clear picture of the flow of direction from the governance to the management to the operations team who will be executing the implementations. Culture, ethics and behavior states good practices that are meant to create, encourage and maintain the desired behavior within the organization. The information enabler supports organizations in decision making process. The diverse features of information determine how effective an organization will attain their stakeholders' needs. Services, infrastructure, and applications include resources that are utilized in the delivery of the IT-related services. People, skills, and competencies give emphasis to the fact that people have the skills and capabilities to create processes and technology.

In an enterprise information security context, COBIT 5 for Information Security recommends that every organization need to define and implement its own information security enablers depending on factors within the enterprise's environment such as; Ethics and culture relating to information security, Applicable laws, regulations and policies, Existing policies and practices, Information security capabilities and available resources.

The COBIT 5 for information security framework describes eight controls namely; risk management, access control, event detection and response, system acquisition and development, operations and procedures, disaster recovery, external parties, regulatory compliance (ISACA, 2012). COBIT 5 for Information Security provides a foundational framework that connects other information security frameworks, good practices and standards.

2.6 Summary of Existing Methodologies

As seen in the previous section, information security assessment is the process of determining how effectively an entity being assessed meets specific security objectives. Information security assessment practices vary between industries, disciplines, and even within the same organization, which has brought about different approaches of assessing information security in an organization. Table 2 below summarized some of existing methodologies reviewed in section 2.4 in respect to existing frameworks and the weakness identified in each assessment methodology.

Table 2*Summary of Information Security Assessment Methodologies*

Information security assessment method	Assessment type	Function	Scope	Framework used	Weakness
Baldrige Cyber Security Excellence Builder (BCEB)	Automated examination	Assess effectiveness of cyber security risk management efforts	Used by organizations that have implemented NIST's Cyber Security framework	NIST Cyber security framework	Limited to Cyber Security Framework.
NIST Framework for cyber security risk self-assessing	Traditional examination	Used to assess cyber security risks during the implementation of NIST cyber security framework. Additionally, it provides a technical guide used to verify that a particular security control meets requirements, at the same time identifying, validating, and assessing a system's exploitable security weaknesses	This method is designed to help organizations implementing the NIST Cyber Security Framework to improve their decision making process about investment priorities.	NIST Cyber security framework	Limited to Cyber Security Framework.
Maryland Health Care Commission (MHCC) Cyber security self-assessment method	Traditional examination	Used to assist small health care providers in identifying gaps and potential risks in their cyber security processes	Designed for health care providers using NIST's Cyber Security Framework	NIST CSF	Limited to Cyber Security Framework use in health care providing organization and cannot be scaled to other organizations
FFIEC Cyber Security Assessment method	Traditional examination	Used by institution's management to identify their risks and determine cyber security preparedness.	Developed by Federal Financial Institutions Examination Council (FFIEC) , to help its institutions identify their risks and determine their	FFIEC Information Technology Examination Handbook, NIST CSF and other cyber security practices	This method is more of a risk assessment technique and is limited to the members of FFIEC

Information security risk assessment	Traditional examination	Used to identify organizations needs regarding information security requirement	cyber security maturity Is part of information security risk management process which focuses on identifying the relevant risks and the appropriate controls for reducing or eliminating these identified risks	Utilized by ISO/IEC 27001 as part of the ISM process	This method is more of a risk assessment method
Fuzzy theory assessment method	Automated examination	Used to evaluate information security controls in organizations	developed with the fuzzy logic toolbox of MATLAB founded on industry accepted cyber security practices	ISO/IEC 27002	Limited to ISO/IEC 27002
Data protection assessment method	Automated interviewing	Used to help organizations assess their compliance with data protection law	Created by Information commissioner office, UK, to help organizations assess their compliance with data protection law	UK data protection law	Limited to assessing compliance to UK data protection law
CS2SAT: The control systems cyber security self-assessment tool	Automated examination	Guides users through a step-by-step process to collect facility-specific control system component information and then makes appropriate recommendations for improving the system's cyber-security posture.	It is a desktop application software developed by department of homeland security national cyber security division to guide in assessment of organization cyber-security posture.	Industry available cyber-security practices	More of a network security control assessment methodology than an organization wide information security assessment methodology

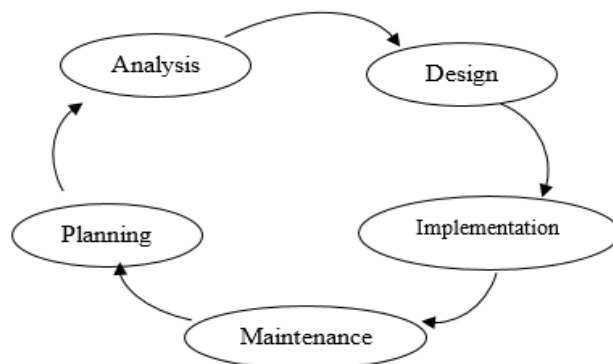
Source: Researcher (2023)

2.7 Model Development Methodologies

Model development is a repetitive process, in which models are derived, tested and built upon until an appropriate model fitting the required specification is achieved. Since conception of computing in the late 1940s, many methods of developing computerized systems and models have emerged. According to Ramic (2015) the systems development life cycle (SDLC) is considered to be the oldest official methodology for creating information systems. The main objective of the SDLC is to track the process of building information systems in a very considered, organized and systematic way, demanding that each phase of the life cycle from the beginning to the end be carried out strictly within the context of the method being used. Examples of SDLC methodologies are, waterfall, agile software development, rapid prototyping, spiral, and incremental software development methodology (Bhuvanewari & Prabakaran, 2013). The SDLC methodology provides a structure of activities for system developers to follow. It involves a set of steps such as planning, analysis, design, and implementation in which each of these phases comes up with a deliverable that will be used by the next phase.

Figure 11

SDLC Activities



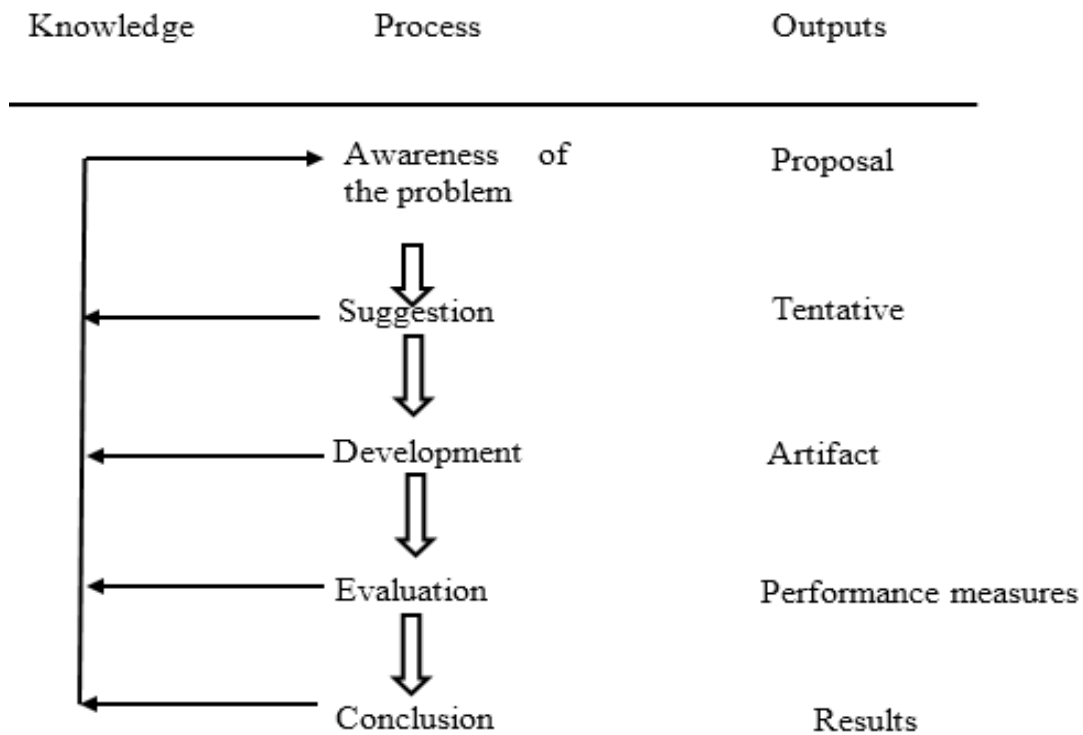
Source: Smith, (2015)

All SDLC methodologies are only concerned with enabling proper development of a system or a model, however most researchers and scholars find these methods limiting because of its inability to guide through the knowledge gathering and problem solving process. In the recent past, scholars and researchers in the field of information technology have adopted other methods from other fields of social and applied sciences to build artifacts that use existing knowledge to solve recurring problems. Design science research is an emerging research paradigm in the field of information systems (Heitkötter & Majchrzak, 2013). The design science research methodology emphasizes on the design and construction of relevant artifacts, such as systems, models, applications, and methods that could hypothetically contribute to the efficiency of information systems in organizations. Design science research purposes on applying existing knowledge to solve motivating and important life problems.

Design science research begins with awareness of the problem, real-world problem identification(Bisandu, 2016). It is followed by the suggestion for a tentative design that is drawn from the existing knowledge base for the identified problem area. The next step is to design the artifact which is derived from the suggested tentative solution, whereby development and evaluation is deductively performed. The design process is iterated back from the awareness, suggestion, development, to evaluation until the real-world situation is improved. Finally, conclusions are drawn, indicating the completion of the development processes.

Figure 12

Design Science Research Process



Source: Karokola, (2012)

Beyond the ability of the conventional SDLC methodologies, DSR methodology contributes to knowledge and design theories away from practical problem solving (Miah & Genemo, 2016).

2.8 Model Evaluation Methodologies

Evaluation is a form of systematic examination of the content, structure and outcomes of programs, artifacts and projects to assess and study the effects, effectiveness and consequences of the innovation, method, policy, practice or service created (Chen et al., 2011). Evaluation is considered as an important act in creation of artifacts that directly contribute to the success of a program/system/artifact/model.

In the field of information systems, evaluation of systems in particular is very beneficial in predicting and assessing potential errors, benefits and risks associated with the implementation and use of the system. There are various methodologies available for information system evaluation each one having its own strengths and weaknesses. Evaluation is categorized in terms of the nature of the evaluation (whether summative or formative) and the strategy adopted in the evaluation (whether goal-based, goal-free or criteria-based).

Formative evaluation is a precise form of evaluation activity that purposes on obtaining feedback during the process of development and implementation of an information system, so as to recommend new methods of improving and supporting the development of the modification (Chen et al., 2011). Alternatively, summative evaluation is a type of evaluation that is carried out after the process of development and implementation is completed, and aims to collect information and feedback to gauge the success, effects, impacts and outcomes of the developed artifact.

Even though formative and summative approaches offer distinct indication on when evaluations should be done, these methodologies do not provide adequate procedures on how evaluation can be completed. Sufficient evaluation cannot be done without identifying some measureable goals. Goal-based evaluation methodology was primarily created as an empirical methodology in which a set of clear, detailed and measurable goals are identified from an organizational/system objectives context prior to evaluation. The artifact is the measured against the predefined goals to determine to what extend are the objectives met. In contrast with the goal-based evaluation methodology, goal-free evaluation is an inferential methodology, which aims at collecting data on the actual effects of an innovation/system/artifact in an environment and then evaluating the

significance of these effects in achieving the established needs of the sociotechnical environment in which the system/artifact/innovation is to create change or solve a problem(Youker, 2010). Alternatively, criteria-based evaluation methodology is whereby evaluation is conducted according to predefined specifications, heuristics, or principles. These parameters are mainly derived from established theories, guidelines, standards or even legal requirements.

2.9 Theoretical Framework

This research uses the Technology-Organization-Environment (TOE) theory to study information security management in organizations so as to understand the key information security controls required to achieve sound information security level in any organization. TOE maintains that the manner in which technological innovations are adopted and implemented in organizations is influenced by the technological, organizational, and environmental contexts surrounding their processes(Awa et al., 2017). These three aspects provide the limits and opportunities for technological adoption, shaping the manner in which an organization assesses its need for an emerging technology.

In information security assessment perspective, the technological context refers to the consistency of existing and new security technologies, able to fulfill the requirements of information security policies and standards, therefore improving organization information security preparedness level(Alkalbani et al., 2014). The organization aspect describes the practices such as communication process and management commitment to upholding organizational security culture hence directing employees' behaviors towards effective information security management. A robust organization culture in terms of information security directly affects employee behaviors and attitudes in observing

information security policies and standards in an organization. The environmental aspect describes the external pressure that forces an organization to attain information security while ensuring availability of services electronically.

The proposed model therefore considers the nine information security controls suggested by international best-practices categorized under the three TOE dimensions of information security implementation; technological, organizational and environmental controls.

2.9.1 Technological Controls

Technological controls focus on the technical controls adopted by organizations to strengthen their information security practices (Alkalbani et al., 2014). Effective organization information security ensures that a reliable and secure technical infrastructure that conform to information security policies requirements are appropriately implemented. For this study the technological controls considered include; Access controls, Network and server security controls, System software security controls, and Data security controls.

Access controls provide policies and procedures for specifying the use of system resources by only authorized users, programs, processes, or other systems (ISO/IEC 27001, 2013). Access control identifies the controls for handling information system accounts, including creating, activating, modifying, reviewing, disabling, and removing accounts. Access controls cover access and flow enforcement issues such as separation of duties, least privilege, unsuccessful login attempts, system use notification, previous logon notification, concurrent session control, session lock, and session termination. They also specify controls set to address the use of portable and remote devices and the implementation of wireless technologies. Access can take several forms, including

viewing, using, and altering specific data or device functions. Access control technologies are filter and blocking technologies designed to direct and regulate the flow of information between devices or systems once authorization has been determined(Stouffer & Abrams, 2015).

Network and server security controls are policies and procedures established to protect organizations data stored in information systems and data in transit(Ismail & Zainab, 2011). Network and security controls ensures authorization of access to data in a network. Some of the safeguarding measures in network and server security include; encryption, access control, firewall, IPS and IDS, and virtual private network for remote access.

System software security controls are policies and procedures established to protect information systems and software against malicious attacks and other risks so that they can continue to function correctly and effectively. System software security controls are implemented to ensure integrity, availability and authenticity of systems and application used in an organization. System software safeguarding measures include; firewalls, antispyware applications, antiviruses among others.

Data security controls are policies and procedures established to secure all organization data whether at rest or in transit(Ismail & Zainab, 2011). Data at rest include data stored in computer systems, databases, portables storage devices including stationary and electronic devices like tapes, disks, etc. whereas data in transit is data that flows in untrusted or public networks and in private networks. Information is one of the most important asset of any organization. Every security management effort undertaken by any organization are centered towards ensuring confidentiality, integrity and availability of information. Therefore, data security controls help to counteract, detect, minimize or

avoid information security risks. Data security controls include; data backup, cryptography, data monitoring, data classification, access controls, portable media protection and disaster recovery plans.

2.9.2 Organizational Controls

Organization controls focus in organizational practices that seek to promote organization security culture and employee perception of information security(Alkalbani et al., 2014). Organizational controls considered in this study include; Human resource security controls, Security awareness, training and education and Information security policies.

Human resource security controls are policies and procedures for personnel position categorization, screening, transfer, penalty, and termination; also addresses third-party personnel security(Stouffer & Abrams, 2015). Employees, contractors and people within an organization are the greatest assets to the organization because of the value they bring in, however, they are considered to be the weakest link in information security (Hassan, 2013).

Awareness, training and education controls provide policies and procedures for ensuring that all users of an information system are provided basic information security education, awareness and training materials before authorization to access the system is granted(Nieles & Dempsey, 2017). These controls ensure that all employees of the organization and contractors receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function (ISO/IEC 27001, 2013). Personnel training must be monitored and documented.

Information security policy controls ensure that a set of policies for information security is defined, approved by management, published and communicated to employees and

relevant external parties (ISO/IEC 27001, 2013). They also ensure that established information security policies are reviewed at planned intervals and significant changes are made to ensure their continuing suitability, adequacy and effectiveness. Information security policy provides management direction and support for information security in accordance with business requirements and relevant laws and regulations. Information security policies include; acceptable use policy, third party and contractor policies, data handling policies among others

2.9.3 Environmental Controls

Environmental controls focus on external and internal measures taken that seek to ensure confidentiality, availability, integrity and assurance of information in government systems and therefore uphold the confidence of all stakeholders including Kenya's citizens in e-governance systems. Environmental controls considered in this study include; Compliance and Physical and environmental security.

Compliance controls seek to ensure that organizations/governments do not violate any criminal or civil law, as well as any statutory, regulatory or contractual obligations, and any other security requirements. These controls ensure that organizations are compliant with legal and contractual requirements as well as organization policies and procedures (ISO/IEC 27001, 2013). ISO/IEC 27001 identify 8 controls under compliance family of controls, they include; Identification of applicable legislation and contractual requirements, intellectual property rights, protection of records, privacy and protection of personally identifiable information, regulation of cryptographic controls, independent review of information security, compliance with security policies and standards, and technical compliance review.

Physical and Environmental controls provide policies and procedures for all physical access to an information system including designated entry and exit points, transmission media, and display media (Nieles & Dempsey, 2017). PE include controls for monitoring physical access, maintaining logs, and handling visitors. Physical and environmental security controls also include controls for the deployment and management of emergency protection controls such as emergency shutdown of the systems, backup for power and lighting, controls for temperature and humidity, and protection against fire and water damage. Physical security measures are designed to reduce the risk of accidental or deliberate loss or damage to plant assets and the surrounding environment. The deployment of physical and environmental security controls is often subject to environmental, safety, regulatory, legal, and other requirements that must be identified and addressed specific to a given environment.

2.10 Research Gap

The literature reviewed showed a need for new information security assessment methodologies that can help county governments in Kenya assess their information security capability to curb evolving information security threats that threaten the success of e-governance initiatives. Since information security management is an ongoing process, new and innovative strategies are needed to provide continuous enhancement of information security in governments.

Analysis of the existing information security assessment methodologies showed that there was no precise methodology that has been developed to address information security assessment problem in Kenya. Although there are numerous information security assessment methodologies available, none of them is a fit for all solution. Most of the assessment methodologies analyzed, are more of risk assessment methods than organization wide information security assessment methods. Furthermore, the available

methods are industry specific and can only be applied to the organizations they are built for. Some of the methods reviewed are meant to assess specific information security controls to check for compliance with industry standards. For instance, the data protection self-assessment method is meant to evaluate the technical controls of an organization information systems, so as to check for compliance with external regulations. Another limitation identified in the existing information security assessment methodologies is limited automation. The available assessment solutions use traditional methods to assess available information assets and information security controls. Information required for assessing information security preparedness level in most of the existing methodologies are collected manually and also analyzed manually.

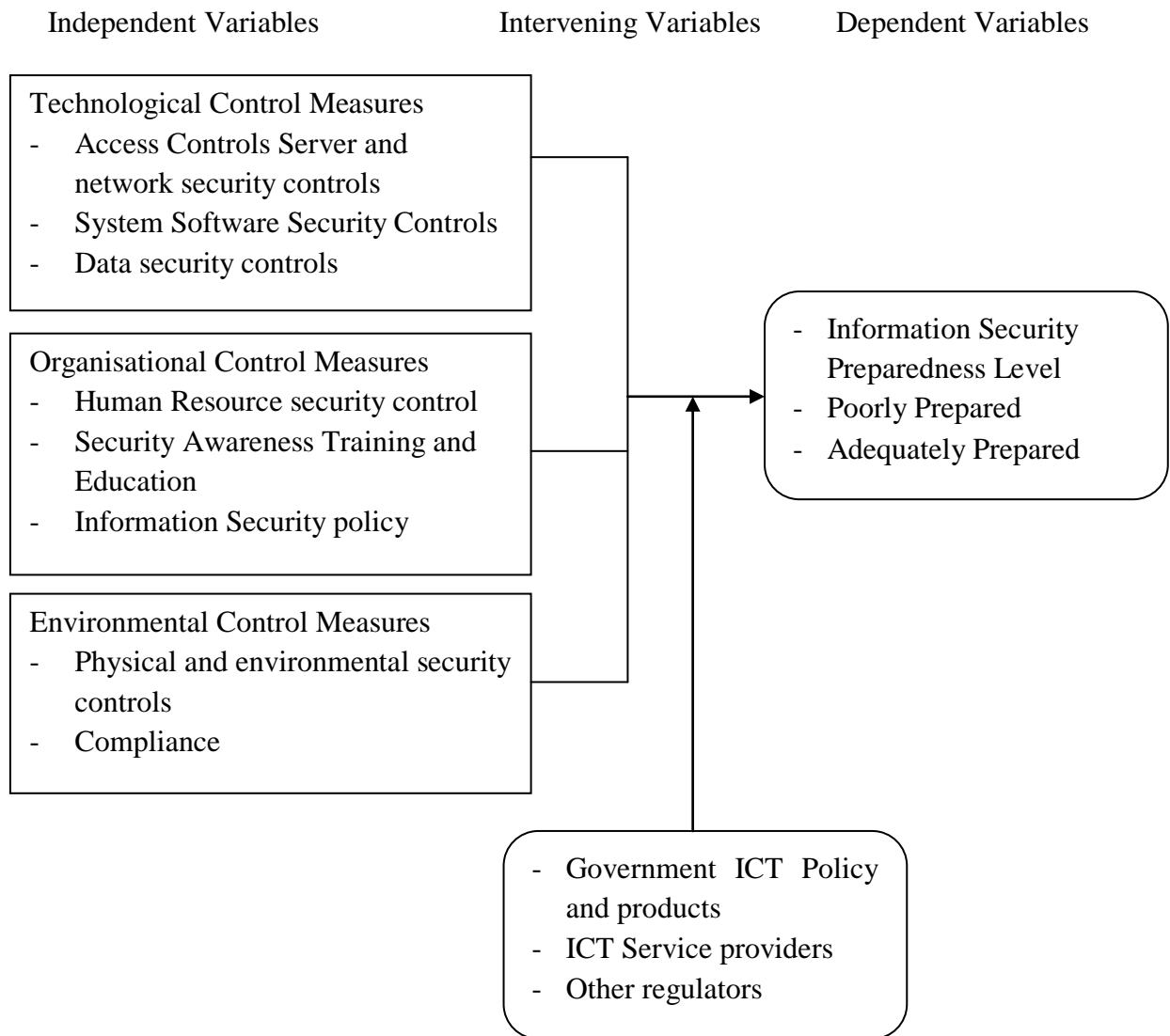
In the light of the information security challenges (discussed in section 2.1.4) faced in implementation of e-governance initiatives, this work recommended a model which is supposed among other things to determine the organizational information security preparedness of Kenya's county governments. The model considered all the aspects of information security control measures—organizational, technological and environmental. Using the recommended information security controls from recognized information security management practices, the study came up with a model that can be used by governments' key personnel to assess their information security preparedness.

2.11 Conceptual Framework

The conceptual framework that guided this study is presented in two stages. First stage showed the conceptual framework indicating independent variables that were used in the derivation of formula for computing information security preparedness level and the dependent variable that is the information security preparedness level. The second stages showed the architectural conceptual framework for implementation of the model

Figure 13

Conceptual Framework



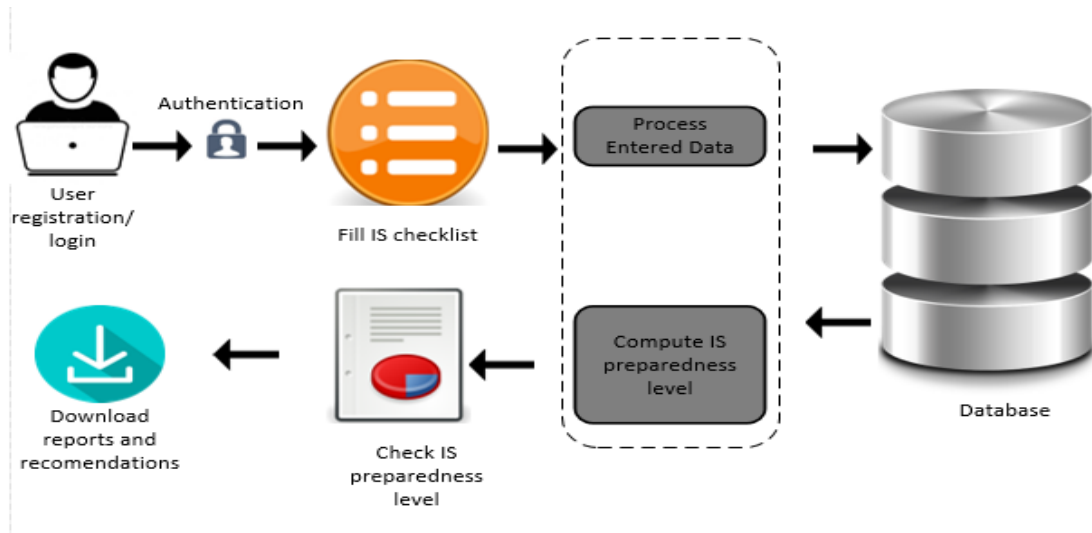
Source: Researcher (2023)

As shown in the Figure 13 above, nine independent variables that affect information security preparedness are grouped under three major categories; technological, organizational and environmental controls. These variables are measured to determine whether the county government is adequately prepared, averagely prepared or poorly prepared in terms of information security. The moderating variables are; government ICT policy and procedures, ICT service providers and other external regulators.

The second stage of the conceptual shows the architectural framework that will guide the development of the model.

Figure 14

Architectural Framework



Source: Researcher (2023)

The model has various modules which include; User login and authentication module which limits access to only authorized users, information security preparedness input module which is in form of an online questionnaire that prompts the information security personnel to provide information security preparedness level of each information security control category he/she is concerned with, information management module for storing information security preparedness information and weights, and information processing module to compute the information security preparedness level from the stored weights and information security preparedness information provided by the users. The model also has a module to display information security preparedness level and also provide an alternative for downloading information security preparedness level report and appropriate recommendations required to achieve acceptable information security level

CHAPTER THREE

RESEARCH METHODOLOGY

3.1 Introduction

This chapter discussed the methods that were used in the development and evaluation of the model for determining information security preparedness level in e-governance in Kenya's county governments. It therefore, outlined the research paradigm, population target, sample size and sampling technique, research instruments, data collection procedure, data analysis and presentation, model development methodology, model evaluation methodology and finally the ethical consideration.

3.2 Research Paradigm

Research paradigm refers to the advancement of scientific practice referring to the people's philosophies and assumptions regarding the world and the nature of knowledge (Antwi & Kasim, 2015). In order to realize the research objectives and satisfactorily address the research questions, the study adopted the design science research method. The study also employed rapid prototyping in the development and designing of the model. With rapid prototyping, the steps of SDLC are intertwined together to reduce the amount of time needed to develop and implement a product.

3.3 Target Population

Population refers to a group of individuals, objects or items that have certain homogenous characteristics from which samples are drawn for measurement and to which the researcher is interested in generalizing the conclusions (Chadwick, 2017). This study was carried out in Uasin Gishu county government. The selected county is part of the 47 county governments that are in Kenya. The research target population included the county executive members, ICT staff, chief information security officers in the

counties and information systems users and custodians within the county governments. Respondents were selected based on their knowledge, experience and roles in e-governance and information security.

3.4 Sampling Procedure

3.4.1 Sample Size

The total population targeted by this research in Uasin Gishu County was 40 people. The table below summarizes the sample frame that was adopted in the selection of survey participants in this study.

Table 3

Target Population

Position	Targeted Number
County executive members	3
ICT staff	10
Chief information security officers	2
Information systems users	15
Information systems custodians	10
Total	40

Source: Researcher (2023)

County executive members targeted were; County director of ICT, Head of Accounts, Head of Human resource sector. Other staffs targeted were; Chief information security officer and his/her assistant, Ten employees working in the IT/ICT department, Fifteen other employees in the county government that use and interact with e-governance systems, Ten Information system custodians who are responsible for e-governance systems like third parties, service providers, storage and cloud service providers and suppliers.

The senior management and county staff were targeted by the study because of their roles in implementation of a security program and because they are the majorly affected people when an e-governance project is implemented.

3.4.2 Sample Technique

The study adopted cluster and simple random sampling methods. Each of the five categories of respondents with knowledge and experience in e-governance that constitute total population were considered as a cluster for the study. Simple random sampling method was used to identify respondents in each cluster.

A census of the target of the total population was conducted. This census attempted to gather information required by the study from all the respondents in the targeted population.

3.5 Research Instrument

This study used structured questionnaire as the primary data collection instrument. Questionnaires were chosen for this study because they are able to collect views and opinions of a large number of respondents within a short time and thus are very appropriate for surveys. Each questionnaire booklet was attached with an introductory letter which contained the research permit, the researcher details, explanation of the research objectives and instructions.

3.6 Data Collection Procedure

Data collection is a means by which information is obtained from the subject of investigation (Creswell & Creswell, 2017). The researcher firstly collected the required research permits from relevant authorities. The questionnaires were administered by the researcher to all the respondents using a drop and pick technique. The researcher

personally distributed by hand the questionnaires to be completed by the selected respondents. Upon completion, the researcher collected the completed questionnaires for analysis.

3.7 The Pilot Study

A total of 5 respondents from Nakuru county government who met the selection criteria were sampled in this survey. Respondents were selected based on their knowledge, experience and roles in e-governance and information security. One person was randomly selected from the five categories (county director of ICT, chief information security officer, ICT staff, information systems users, information systems custodian) of the total population. Pilot test was conducted to detect weakness in design and instrumentation. Cronbach's alpha (α) was used to measure the reliability of the instruments used. To avoid misrepresentation and minimize errors, the researcher did a pre-test of the questionnaires before the actual data collection. The results of the pilot study informed improvement of research instruments that enhanced validity and reliability but they were not used in the data analysis.

3.7.1 Reliability Analysis

Reliability Analysis was analyzed using Cronbach's Alpha coefficient. The finding show that all the indicators had a Cronbach's Alpha above the threshold of 0.7. This indicated that all the variables were reliable.

Table 4*Reliability Analysis for the Pilot Study*

Indicators	Cronbach's Alpha	No of Items	Decision
Access controls	0.816	5	Reliable
System software security safeguarding measures	0.924	5	Reliable
Network security and server security safeguarding measures	0.821	5	Reliable
Data security safeguarding measures	0.756	5	Reliable
Human resource security safeguarding measures	0.815	5	Reliable
Information security policy	0.780		Reliable
Awareness creation, training and education	0.857		Reliable
Compliance	0.733	5	Reliable
Physical and environmental security	0.752	5	Reliable
Information security preparedness	0.811	9	Reliable

Source: Researcher (2023)

3.8 Data Analysis

Data analysis refers to executing what has been collected in a study and making deductions and inferences. This study collected large amounts of data regarding the variables under study, thus the need to summarize data and information collected arose. It included analysis of data to summarize the essential features and relations of data in order describe the state of affairs and determine patterns of behavior and particular outcomes. Before processing the responses, the completed questionnaires were edited for completeness and consistency. The data were then coded to enable the responses to be grouped into various categories. Analysis of the findings was done using descriptive statistics and inferential statistics in the form of frequency distributions, percentages

measures of central tendencies and positions, regression and correlation analysis to establish any emerging patterns which were presented in tables. Pearson correlation was used to test the nature of relationship among the variables. The analysis and presentation was done with the aid of IBM SPSS Version 20 (Statistical Package for the Social Sciences).

3.9 Model Development

This study adopted design science research methodology to realize the research objectives and satisfactorily address the research questions. Design science research methodology is used to create innovations and ideas that define technical capabilities and products through which the development process of artifacts can be effectively and efficiently accomplished (Karakola, 2012).

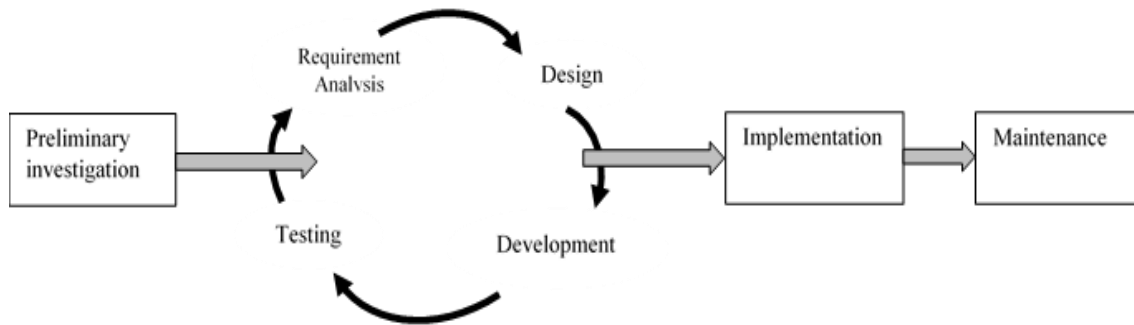
Based on the design science research methodology, the design and development of the model was divided into the following steps;

- i. Awareness of the real-world problem and understanding the complexity of the problem
- ii. Suggestions of a tentative design
- iii. Development the OISP model
- iv. Evaluation of the OISP model

Rapid prototyping methodology was used to implement the model. The goal of rapid prototyping is to provide a system with overall functionality within a minimum time and budget.

Figure 15

Rapid Prototyping Development Activities



Source: Smith, (2015)

In rapid prototyping, interactive models are developed which can be quickly replaced or changed in line with the users' feedback. The development of a model is useful, as it allow users to visualize the system and provide feedback on it.

Rapid prototyping is associated with many tangible and abstract advantages, which include providing users with a tangible feel of the functionality of the system, and proper clarity of the proposed system, therefore users can suggest changes and modifications to be made. The models created by rapid prototyping relate highly with the final product and therefore users can get a better understanding of the system being developed. Also, rapid prototyping allows rapid development of interactive models to users, this iteration between development team and client provides a very good and conducive environment to resolve unclear objectives.

The researcher first did a preliminary investigation in order to identify the basic requirements of the OISP model such as input and output information desired. Iteratively, the researcher then designed the user interfaces and developed the system. The model was deployed online to allow end users to review and provide feedback on

potential additions or changes to the system. Finally the system was tested and evaluated to determine its ability to meet the predefined objectives.

3.10 Model Evaluation

Evaluation is one of the most important steps in system development (Otero, 2014). It provides essential feedback to the system development and quality assurance process. There are a number of evaluation methods that could be used for evaluating a framework or a prototype or a system as discussed in chapter two. The model was tested by using a goal-based evaluation approach which determines the extent at which the model was achieving its predefined objectives. The predefined objectives of the model are;

- i. The model should have a working user login and authentication model to restrict access to the model hence enhancing security of the model
- ii. The model should be able to retrieve assessment questions from the OISP database and present them to the user in a Likert scale layout and also allow the user to submit duly filed assessment form to the database.
- iii. The model should be able compute the preparedness level as per submitted user scores and present the results to the user in percentage
- iv. The model should be able to retrieve reports on assessment scores and recommendations and allow the user to download the output into a portable and printable document format.
- v. The model is supposed to allow registration of new users as per their roles and responsibilities in information security management and also allow assignment of assessment questions as per their roles and responsibilities.

3.11 Ethical Consideration

Ethics is an important issue when conducting research. This relates to moral standards that the researcher should consider in all research methods in all stages of the research design. The researcher sought approval from the University to conduct the study, and permission from the ethics agency. The researcher followed three principles of the Belmont Report, namely beneficence, respect for human dignity as well as justice while conducting the research. All the respondents that participated in this study were treated in an ethical manner not only by respecting their decisions and protecting their anonymity, but also by making efforts to secure their information. The researcher understood that plagiarism is an offence against intellectual rights, and therefore plagiarism was avoided by acknowledging all used sources by referencing. Also, confidentiality of the data collected from the county of study was ensured by providing anonymity to sources of information, including coding of names where necessary.

CHAPTER FOUR

DATA ANALYSIS, PRESENTATION AND DISCUSSION

4.1 Introduction

This chapter presents the analyzed data. It begins with response rate of the study, general background information, descriptive and correlation analyses. It further proceeds to describe how the model was developed and evaluated.

4.1.1 Response Rate

A response rate is a mathematical formula that is calculated by survey researchers and is used as an instrument to understand the degree of success in obtaining completed interviews from a sample. The study distributed 40 questionnaires and all were filled and collected. This gave a response rate of 100%.

4.1.2 General Background Information

This section analyzed data relating to the respondents' job title, academic qualification and work experience. The results are presented subsequently.

Table 5

Job Title

Characteristic	Frequency	Percent
Chief Information security officers	2	5.0
County executive members	3	7.5
ICT staff	10	25.0
Information system custodians	10	25.0
Information system users	15	37.5
Total	40	100.0

Source: Researcher (2023)

The study found that information users were the majority (37.5%), Information system custodians and ICT staff were 25% respectively. The Chief Information security officers and County executive members were 5% and 7.5% respectively.

Table 6

Highest Academic Qualification

Characteristic	Frequency	Percent
Degree	35	87.5
Masters	4	10.0
PhD	1	2.5
Total	40	100.0

Source: Researcher (2023)

It was acknowledged that majority were degree holders (87.5%), Masters (10%) and 2.5% PhD holders.

Table 7

How long have you been Working for this county?

Range	Frequency	Percent
2 – 5 years	27	67.5
More than 5 years	13	32.5
Total	40	100.0

Source: Researcher (2023)

Respondents reported that they had 2-5 years' work experience in county government while 32.5% had more than 5 years in county government. This respondent's work experience was seen to provide valuable data for the study.

Respondents were further asked to indicate their work experience in Information Technology. The results are presented in Table 8.

Table 8

Work Experience in Information Technology

Range	Frequency	Percent
11 – 15 years	22	55.0
16 – 20 years	18	45.0
Total	40	100.0

Source: Researcher (2023)

It was noted that 55% of Respondents reported that they had worked between 11 – 15 years while 45% up to 20 years. This suggests that the majority of the respondents had rich experience in the field of information technology and hence they were in a position to understand the problem under investigation.

4.2 Data Analysis

Descriptive analysis such as percentages was used to examine distributional patterns of variables under study. The independent variables were descriptively analyzed and the findings presented in subsequent tables. The chi-square (χ^2) values indicated in table 9 to table 17 is the chi-square goodness of fit which shows how data was distributed across the distributional categories. The p-values also indicated the relationship between the observed values and the expected values of the different variables analyzed, however does not indicate the significance of the variable analyzed. P-values less than 0.05 shows that there was a significant difference between the observed values and expected values while that greater than 0.05 shows that there was no significant difference between the observed values and expected values.

4.2.1 Technological Controls

4.2.1.1 Access Controls

Table 9

Access Controls

Statement	X1	X2	X3	X4	X5	χ^2	P
There is a documented access control policy that is communicated appropriately	15.0%	15.0%	50.0%	20.0%	0.0%	13.60	0.004
There are controls in place to ensure users only have access to the network resources and that they have been specially authorized to use as required for their duties	0.0%	30.0%	50.0%	20.0%	0.0%	5.60	0.061
There is formal user access registration process and a formal user access provisioning process for assigning access rights for all user types and services	12.5%	47.5%	40.0%	0.0%	0.0%	8.15	0.017
There is a process to ensure user access rights are removed on termination of employment or contract, or adjusted upon change of role	0.0%	37.5%	32.5%	12.5%	7.5%	6.80	0.079
Access to information and application system functions are restricted in line with the access control policy	0.0%	30.0%	32.5%	37.5%	0.0%	0.35	0.839

Key: X1= Not implemented; X2= only some part has been implemented; X3= Implemented but has not been reviewed; X4= Implemented and reviewed on regular basis; X5= fully implemented and recognized as good for information security; χ^2 =chi-square

Source: Researcher (2023)

The study indicated that 15% asserted that documented access control policy has not been implemented while some 15% of respondents reported that only some part has been implemented. Similarly, half of the respondents (50%) affirmed that access control

policy have been implemented but has not been reviewed. This situation could pose an information security threats in organizations.

This position was confirmed by another 50% who assert that there are controls in place to ensure users only have access to the network resources and that they have been specially authorized to use as required for their duties, which have been implemented but has not been reviewed.

Respondents affirmed that user access registration process and a formal user access provisioning process for assigning access rights for all user types and services have some part being implemented. It was worth noting that up to 12.5% maintained that user access registration process and a formal user access provisioning process had not been implemented. This also could pose an information security threat in the organization.

On the other hand, 17.5% of respondents agreed that there is a process to ensure user access rights are removed on termination of employment or contract, or adjusted upon change of role which was fully implemented and recognized as good for information security. Despite this view, 37.5% assert that only some part has been implemented while 32.5% reported that the process to ensure user access rights are removed on termination of employment was implemented but has not been reviewed.

It was also noted that 30% of the respondents claimed that the access to information and application system functions in county government were restricted in line with the access control policy safeguarding measure, had been partially implemented while another 32.5% stated that the said safeguarding measure had been fully implemented but not reviewed, while another 37.5% acknowledged that the said measure was fully implemented and regarded as a good information security measure.

These findings imply that, there are disintegrated information security management efforts across different departments in county governments as observed by Mohammad (2012). The findings show that access controls are not implemented consistently by different departments in county governments.

4.2.1.2 System Software Security Safeguarding Measures

System software security safeguarding measures was analyzed and presented in Table 10.

Table 10

System Software Security Safeguarding Measures

Statement	X1	X2	X3	X4	X5	χ^2	P
There are established procedures which list all requirements with regard to outsourcing any county Information Systems service or activities.	0.0%	47.5%	32.5%	20.0%	0.0%	4.55	0.103
There are antispyware, anti-phishing and cleanup software solutions to detect, prevent and remove any spyware threats, phishing attacks and trashed files regularly.	12.5%	32.5%	5.0%	30.0%	20.0%	10.75	0.030
There is a rollback software to keep track and record any changes made to the computers and allow the system to be restored to its original state from any chosen point in time.	2.5%	15.0%	50.0%	32.5%	0.0%	20.60	0.000
There is a web filtering software to prevent access to inappropriate materials or sites.	17.5%	30.0%	50.0%	0.0%	2.5%	19.40	0.000
There is an application firewall is used for mobile laptops that connect to the county's LAN	0.0%	17.5%	50.0%	32.5%	0.0%	6.35	0.042

Key: X1= Not implemented; X2= only some part has been implemented; X3= Implemented but has not been reviewed; X4= Implemented and reviewed on regular basis; X5= fully implemented and recognized as good for information security; χ^2 =chi-square

Source: Researcher (2023)

Regarding system software security safeguarding measures, 20% of respondents affirmed that there are established procedures which list all requirements with regard to outsourcing any county information systems service or activities which was implemented and reviewed on regular basis. However, 47.5% avow that only some part has been implemented. Equally, 32.5% reported that it had been implemented but has not been reviewed. Therefore, this could imply that there could be a problem with information security in some departments.

It was noted that half of respondents (50%) state that there is antispayware, anti-phishing and cleanup software solutions to detect, prevent and remove any spyware threats, phishing attacks and trashed files regularly which was implemented and reviewed. This is a good sign of security preparedness of an organization. However, 12.5% maintained that the cleanup software solutions were not implemented while 32.5% aver that only some part has been implemented. Also, 32.5% agreed that there is a rollback software to keep track and record any changes made to the computers and allow the system to be restored to its original state from any chosen point in time and was implemented and reviewed on regular basis.

Furthermore, 15.0% reported that the rollback software had only some part has been implemented. Surprisingly, 2.5% avow that the rollback software had not implemented at all. The finding also revealed that half of the respondents (50%) asserted that there is a web filtering software to prevent access to inappropriate materials or sites as well as that there is an application firewall is used for mobile laptops that connect to the county's LAN which were implemented but has not been reviewed. However, 30.7% and 17.5% reported that web filtering software and application firewall had some part been implemented.

These findings on system software security safeguarding measures shows how different departments dealing with information security management in Uasin Gishu county are not aware and ignorant of existing information security practices adopted, bringing inconsistencies in implementation and updating of information security measures (Hassan, 2013). This implies that measures used to safeguard system soft wares are not communicated causing impartiality in the implementation and maintenance of these measures.

4.2.1.3 Network Security and Server Security Safeguarding Measures

Network security and server security safeguarding measures was analyzed and presented in Table 11.

Table 11*Network Security and Server Security Safeguarding Measures*

Statement	X1	X2	X3	X4	X5	χ^2	P
Firewall to protect the internal network from external threats and with virtual private network installed for remote and wireless access connections	0.0 %	30.0 %	40.0 %	10.0 %	20.0%	8.00	0.046
Use of wireless security products to secure the county wireless network. (Use of default passwords on wireless access points, network ID, wireless intrusion detection systems, wired equivalency protocol (WEP) encryption, MAC address filtering or virtual private networking (VPN)	0.0 %	17.5 %	27.5 %	55.0 %	0.0%	9.05	0.011
There is an authentication system to prevent unauthorized access to the county's server.	0.0 %	37.5 %	40.0 %	20.0 %	2.5%	14.60	0.002
There is routine backup for the data, safe storage of hard copy of server hardware specifications, installation information, installation software and passwords at an offsite location.	0.0 %	0.0 %	80.0 %	20.0 %	0.0%	14.40	0.000
The server is placed in a secure location, such as in a lockable cage, a locked room and place it with environmental controls.	12.5 %	47.5 %	20.0 %	20.0 %	0.0%	11.40	0.010

Key: X1= Not implemented; X2= only some part has been implemented; X3= Implemented but has not been reviewed; X4= Implemented and reviewed on regular basis; X5= fully implemented and recognized as good for information security; χ^2 =chi-square.

Source: Researcher (2023)

It was observed that 40.0% declared that firewall to protect the internal network from external threats and with virtual private network installed for remote and wireless access connections was implemented but has not been reviewed while 30% reported that it had been implemented and reviewed. On the other hand, another 30% avers that only some part has been implemented.

Similarly, 55.0% affirmed that use of wireless security products to secure the county wireless network implemented and reviewed on regular basis and supported by 27.5% reported that it was implemented but has not been reviewed. Conversely, up to 17.5% of respondents asserts that only some part has been implemented. This may not be good for security of organization information.

Furthermore, 40.0% reported that there is an authentication system to prevent unauthorized access to the county's server. This view was supported by 25% who maintained that implemented and reviewed and recognized as good for information security. Despite this development, 37.5% reported that only some part has been implemented hence this could expose these organizations to external threats. Moreover 80.0% avers that there is routine backup for the data, safe storage of hard copy of server hardware specifications, installation information, installation software and passwords at an offsite location (implemented but has not been reviewed) while 20% avow that it had been implemented and reviewed on regular basis.

Finally, the study revealed that 2.0% affirm that the server is placed in a secure location, such as in a lockable cage, a locked room and place it with environmental controls. This position had been implemented and reviewed on regular basis. Nevertheless, 12.5% of respondents' assert that they had not implemented as 47.5% argue that only some part has been implemented. These finding show that despite the availability of measures for safeguarding network and server infrastructure, few employees are aware of the status of implementation of these measures in Uasin Gishu County. This insinuate that the personnel in Uasin Gishu county are rarely taught and educated on implemented information security measures meant to secure their networks and servers.

4.2.1.4 Data Security Safeguarding Measures

Network security and server security safeguarding measures was analyzed and presented in Table 12.

Table 12

Data Security Safeguarding Measures

Statement	X1	X2	X3	X4	X5	χ^2	P
There are data classification, retention and destruction procedures for handling county data, media or materials that contain county sensitive information	17.5%	20.0%	17.5%	45.0%	0.0%	8.60	0.035
There are procedures on intellectual property rights and copyrights in controlling and protecting any digital works or resources that are stored, transmitted, accessed, copied or downloaded via the county information systems	17.5%	37.5%	12.5%	32.5%	0.0%	6.80	0.079
There are policies on sharing, storing and transmitting of county data via ISPs, external networks or contractors' systems.	0.0%	47.5%	32.5%	20.0%	0.0%	4.55	0.103
Use of cryptography techniques, hardware & software tokens and single sign on systems to control data access to the county internal and remote computer systems	30.0%	0.0%	37.5%	32.5%	0.0%	0.35	0.839
Vital County's business information or records are regularly backed up and stored in a different site.	0.0%	50.0%	30.0%	20.0%	0.0%	5.60	0.061

Key: X1= Not implemented; X2= only some part has been implemented; X3= Implemented but has not been reviewed; X4= Implemented and reviewed on regular basis; X5= fully implemented and recognized as good for information security; χ^2 =chi-square.

Source: Researcher (2023)

It was noted that 45.0% of respondents agreed that there are data classification, retention and destruction procedures for handling county data, media or materials that contain county sensitive information which were implemented and reviewed on regular basis. However, 17.5% affirmed that data classification, retention and destruction procedures had not been implemented. This implies that information security of organization could be in danger.

In addition, 32.5% of respondents declare that there are procedures on intellectual property rights and copyrights in controlling and protecting any digital works or resources that are stored, transmitted, accessed, copied or downloaded via the county information systems. These procedures on intellectual property rights and copyrights were implemented and reviewed on regular basis. Despite this development, 17.5% avow that it had not been implemented. This also suggests that the safety of organizations' data could be under a threat.

Moreover, 20.0% affirmed that there are policies on sharing, storing and transmitting of county data via ISPs, external networks or contractors' systems as implemented and reviewed on regular basis. Remarkably, nearly half (47.5%) avow that only some part has been implemented while 32.5% had implemented but has not been reviewed.

The findings also indicated that 32.5% affirmed that use of cryptography techniques, hardware & software tokens and single sign on systems to control data access to the county internal and remote computer systems had been implemented and reviewed on regular basis. However, 30.0% reported that it had not been implemented in their department. This implies that the security preparedness was in problems in most of the departments.

Finally, 50.0% of respondents agreed that vital County's business information or records are regularly backed up and stored in a different site though partly being implemented. While 20% maintained that was being implemented and reviewed on regular basis. This will therefore improve on security of the data in the County's department.

On data protection, the findings showed that Uasin Gishu County have deployed few measures to safeguard their data. Different departments employ different measures to protect their data creating inconsistencies in the efforts to safeguard data.

4.2.2 Organization Controls

This was the second independent variable. The analysis is presented subsequently.

4.2.2.1 Human Resource Security Safeguarding Measures

Table 13

Human Resource Security Safeguarding Measures

Statement	X1	X2	X3	X4	X5	χ^2	P
Background verification checks carried out on all new candidates for employment and approved by appropriate management authority	10.0%	30.0%	22.5%	32.5%	5.0%	11.75	0.019
All employees and contractors sign confidentiality and non-disclosure agreements	17.5%	35.0%	20.0%	27.5%	0.0%	3.00	0.392
County executive members are engaged in driving security within the county and encourage, all employees and contractors to apply security in accordance with established policies and procedures	5.0%	45.0%	40.0%	5.0%	5.0%	34.00	0.000
There are formal disciplinary procedures which allows the organization to take action against employees who have committed an information security breach. Verbal warning, written warning, suspension or dismissal.	0.0%	12.5%	70.0%	10.0%	7.5%	43.40	0.000
There is a documented process for terminating or changing employment duties and is communicated to the employees and/or contractors	5.0%	42.5%	22.5%	25.0%	5.0%	19.75	0.001

Key: X1= Not implemented; X2= only some part has been implemented; X3= Implemented but has not been reviewed; X4= Implemented and reviewed on regular basis; X5= fully implemented and recognized as good for information security; χ^2 =chi-square.

Source: Researcher (2023)

Regarding Human Resource Security safeguarding measures, 37.5% reported that background verification checks carried out on all new candidates for employment and approved by appropriate management authority was implemented and reviewed. By the same token, 30.0% reported that only some part has been implemented. It was however

observed that 10.0% had not implemented which could be a cause of concern to this study.

Additionally, 27.5% reported that all employees and contractors sign confidentiality and non-disclosure agreements. This view was supported by 20.0% who affirmed that confidentiality and non-disclosure agreements had been implemented but has not been reviewed. However, 17.5% stated that they had not implemented at all.

It was documented that only 10.0% asserted that County executive members are engaged in driving security within the county and encourage, all employees and contractors to apply security in accordance with established policies and procedures. On the other hand, 40.0% reported that the statement had been implemented but has not been reviewed. On contrary, 45.0% posits that only some part has been implemented and while 5.0% revealed that it had not implemented. This could affect security preparedness by departments.

It was noted that 70.0% agreed that there are formal disciplinary procedures which allows the organization to take action against employees who have committed an information security breach. Verbal warning, written warning, suspension or dismissal have been implemented but has not been reviewed. Furthermore, 17.5% had implemented and reviewed formal disciplinary procedures. On the other hand, 12.5% suggests that these procedures had not been implemented in their department.

Lastly, 42.5% affirmed that there is a documented process for terminating or changing employment duties and is communicated to the employees and/or contractors though only some part has been implemented. Similarly, 5.0% reported that termination process had not been implemented.

4.2.2.2 Information Security Policy

Table 14

Information Security Policy

Statement	X1	X2	X3	X4	X5	χ^2	P
There are policies on access control authentication and authorization practices for using the county Information Systems.	17.5%	35.0%	15.0%	32.5%	0.0%	5.00	0.172
There are policies on protection of county assets to protect your county's hardware, software, data and people.	0.0%	50.0%	32.5%	17.5%	0.0%	6.35	0.042
There are polices on reporting, notification and response of Information Systems security events to affected parties such as citizens, law enforcement, and business partners.	32.5%	0.0%	35.0%	32.5%	0.0%	0.05	0.975
Policies on acceptable use of wireless devices in your county such as laptops and hand phones, workstations, emails, databases, intranet and Internet in your county	0.0%	17.5%	55.0%	27.5%	0.0%	9.05	0.011
Procedures for update and review existing information security policies	0.0%	10.0%	50.0%	40.0%	0.0%	10.40	0.006

Key: X1= Not implemented; X2= only some part has been implemented; X3= Implemented but has not been reviewed; X4= Implemented and reviewed on regular basis; X5= fully implemented and recognized as good for information security; χ^2 =chi-square.

Source: Researcher (2023)

Respondents agreed that there are policies on access control authentication and authorization practices for using the county Information Systems (32.5%). This policy was had been implemented and reviewed on regular basis. Similarly, 35.0% reported that only some part has been implemented. On the other hand, 17.5% reported that it had not

been implemented. This clearly shows that some departments lacked a well functional information security policy.

Respondents also agreed that there are policies on protection of county assets to protect their county's hardware, software, data and people (50.0%). In this policy only some part has been implemented while up to 32.5% affirmed that it had been implemented but has not been reviewed. It was also affirmed by 17.5% that the policy had been implemented and being reviewed on regular basis. The study further indicated that 32.5% affirmed that there are policies on reporting, notification and response of Information Systems security events to affected parties such as citizens, law enforcement, and business partners. In addition, 35.0% reported that the policy had been implemented but has not been reviewed. However, 32.5% confirmed that the policy had not implemented.

Respondents also agreed that there are policies on acceptable use of wireless devices in their county such as laptops and hand phones, workstations, emails, databases, intranet and Internet (27.5%). This policy was under review on regular basis. It was also reported by 55.0% that the policy had been implemented but has not been reviewed. On the other hand, 17.5% aver that only some part has been implemented. This could affect the overall security preparedness as regards to organizations' information. Respondents agreed that there are procedures for update and review existing information security policies (40.0%). Similarly, 50.0% affirmed that the policy had been implemented but has not been reviewed. On the other hand, only 10.0% aver that only some part of the policy had been implemented. This implies that information security of organization could be vulnerable to external threats.

4.2.2.3 Awareness Creation, Training and Education

Table 15

Awareness Creation, Training and Education

Statement	X1	X2	X3	X4	X5	χ^2	P
All staff at various levels are made aware of their responsibilities with regard to protecting the county's Information Systems' security and are also regularly trained to report any security breach incidences.	12.5%	35.0%	45.0%	7.5%	0.0%	15.40	0.002
All staff at various levels receive appropriate information security trainings and education on regular basis and routinely updated on county information security policies and procedures	0.0%	22.5%	65.0%	7.5%	5.0%	37.00	0.000
Information security awareness trainings is mandatory to all staff and patrons at various levels.	10.0%	50.0%	35.0%	5.0%	0.0%	21.60	0.000
There are balanced set of key performance indicators (KPIs) and metrics used to provide the real insight into the effectiveness of security awareness programs.	0.0%	45.0%	32.5%	10.0%	12.5%	13.40	0.004
There are positive supports and commitments from the top management to coordinate the implementation of Information Systems' security controls in your county. (such as allocation of budget, strong interest and active involvements)	0.0%	37.5%	27.5%	35.0%	0.0%	0.65	0.723

Key: X1= Not implemented; X2= only some part has been implemented; X3= Implemented but has not been reviewed; X4= Implemented and reviewed on regular basis; X5= fully implemented and recognized as good for information security; χ^2 =chi-square.

Source: Researcher (2023)

Respondents agreed that all staff at various levels are made aware of their responsibilities with regard to protecting the county's information Systems' security and are also

regularly trained to report any security breach incidences (45.0%). Despite development, this 12.5% revealed that the practice had not been implemented in their department. Furthermore, 65.0% of respondents' assert that all staff at various levels receive appropriate information security trainings and education on regular basis and routinely updated on county information security policies and procedures while 22.5% reports that only some part has been implemented. Moreover, 50.0% of respondents suggest that information security awareness trainings are mandatory to all staff and patrons at various levels. However, 10.0% affirm that information security awareness has not been implemented.

It was seen that 12.5% agreed that there are balanced set of key performance indicators (KPIs) and metrics used to provide the real insight into the effectiveness of security awareness programs while 45.0% had a different opinion.

Respondents agreed that there are partly positive and commitments from the top management to coordinate the implementation of Information Systems' security controls in their county (35.0%) which was implemented and reviewed regularly. On the other hand, 37.5% reports that only some support from management was yet to be realized.

4.2.3 Environmental Controls

This was the third independent variable was analyzed and presented subsequently.

4.2.3.1 Compliance

Table 16

Compliance

Statement	X1	X2	X3	X4	X5	χ^2	P
The county has identified and documented all relevant legislative, regulatory or contractual requirements related to security	17.5%	10.0%	50.0%	22.5%	0.0%	14.60	0.002
All the records within the county are protected from loss, destruction, falsification and unauthorized access or release in accordance with legislative, regulatory, contractual and business requirements	10.0%	37.5%	17.5%	35.0%	0.0%	8.60	0.035
The county protects personal data in accordance with relevant legislation	17.5%	17.5%	40.0%	15.0%	10.0%	10.75	0.030
The county ensures that the implementation of security controls and information security is subject to regular independent reviews	0.0%	35.0%	32.5%	15.0%	17.5%	5.00	0.172
The county conducts technical compliance reviews of e-governance information systems regularly	0.0%	27.5%	32.5%	40.0%	0.0%	0.95	0.622

Key: X1= Not implemented; X2= only some part has been implemented; X3= Implemented but has not been reviewed; X4= Implemented and reviewed on regular basis; X5= fully implemented and recognized as good for information security; χ^2 =chi-square.

Source: Researcher (2023)

Regarding Human Resource Security safeguarding measures, 22.5 % reported that the county has identified and documented all relevant legislative, regulatory or contractual requirements related to security. The contractual requirements were being implemented and reviewed on regular basis. However, 17.5% assert that the contractual requirements

not implemented could affect security position of information and data in the organization.

It was noted that 35.0% affirm that all the records within the county are protected from loss, destruction, falsification and unauthorized access or release in accordance with legislative, regulatory, contractual and business requirements. This view was further upheld by 37.5% who reports that some part of the process has been implemented. On the other hand, 10.0% maintain that the process had not been implemented.

Respondents aver that the county protects personal data in accordance with relevant legislation with 25% affirming that the practice had been implemented and reviewed. This view was further upheld by 40.0% who reported that the practice had been implemented. However, 17.5% state that the practice had not implemented.

In the same way, 17.5% agree that the county ensures that the implementation of security controls and information security is subject to regular independent reviews. This view was corroborated by 15.0% that the security controls had been Implemented and reviewed. Despite this development, 35.0% aver that only some part has been implemented.

Respondents affirmed that the county conducts technical compliance reviews of e-governance information systems regularly (40.0%). Equally, 32.5% support that county conducts technical compliance reviews of e-governance information systems. Regardless of this advances, 27.5% opines that only some part has been implemented. This could be a cause of concern in information security in organizations.

4.2.3.1 Physical and Environmental Controls

Table 17

Physical and Environmental Security

Statement	X1	X2	X3	X4	X5	χ^2	P
Lightning protectors and surge protectors to protect any valuable machines or equipment from lighting strikes, voltage spikes and surges	5.0%	22.5%	50.0%	22.5%	0.0%	16.60	0.001
Security guards to monitor people entering and leaving the county buildings and sites	0.0%	42.5%	17.5%	40.0%	0.0%	4.55	0.103
Use of automatic sprinkler systems, smoke detectors, fire extinguishers and fireproof installations in the county buildings to detect and prevent fires, toxic chemical spills and explosions	5.0%	15.0%	52.5%	27.5%	0.0%	20.20	0.000
Use of magnetic stripe swipe cards, electronic lock, proximity cards, bar code card or biometrics to secure and control access to restricted county areas	10.0%	22.5%	32.5%	35.0%	0.0%	6.20	0.102
Air conditionings to stabilize the temperature & humidity within the county building	12.5%	22.5%	50.0%	15.0%	0.0%	14.20	0.003

Key: X1= Not implemented; X2= only some part has been implemented; X3= Implemented but has not been reviewed; X4= Implemented and reviewed on regular basis; X5= fully implemented and recognized as good for information security; χ^2 =chi-square.

Source: Researcher (2023)

According to table 15, respondents opined that there were lightning protectors and surge protectors to protect any valuable machines or equipment from lighting strikes, voltage spikes and surges (72.5%). This finding was also affirmed by 22.5% of respondents. Notwithstanding this view, only 5.0% reported that it had not been implemented. Furthermore, 40.0% reported that there were security guards to monitor people entering

and leaving the county buildings and sites and was supported by 17.5%. However, 42.5% asserted that only some part of security guards has been implemented.

Moreover, 52.5% agreed that use of automatic sprinkler systems, smoke detectors, fire extinguishers and fireproof installations in the county buildings to detect and prevent fires, toxic chemical spills and explosions while 27.5% also supported the statement. It was noted that 5.0% reported that these detectors had not been implemented. It was noted that 35.0% agreed that there was use of magnetic stripe swipe cards, electronic lock, proximity cards, bar code card or biometrics to secure and control access to restricted county areas. Also, 32.5% confirmed the position while 10.0% affirm that these measures had not been implemented. Finally, up to 15.0% agreed that there was air conditioning to stabilize the temperature & humidity within the county building. It was noted by 50.0% that there was air conditioning to stabilize the temperature. This position supported by 22.5% of respondents. However, 12.5% of respondents aver that the appliances had not been implemented in their department.

4.2.4 Information Security Preparedness Indicators

The dependent variable was analyzed in terms of the following indicators.

Table 18*Information Security Preparedness Indicators*

Statement	X1	X2	X3	X4	X5	χ^2	P
Access controls	0.0%	50.0%	32.5%	17.5%	0.0%	6.35	0.042
Server and network security	15.0%	35.0%	0.0%	32.5%	17.5%	5.00	0.172
System software security	0.0%	17.5%	50.0%	32.5%	0.0%	6.35	0.042
Data security	0.0%	47.5%	17.5%	35.0%	0.0%	5.45	0.066
Human Resource Security	0.0%	15.0%	67.5%	17.5%	0.0%	21.05	0.000
Security awareness, training and education	15.0%	32.5%	17.5%	35.0%	0.0%	5.00	0.172
Information security policy	17.5%	17.5%	50.0%	15.0%	0.0%	13.40	0.004
Physical and environmental security	0.0%	17.5%	35.0%	30.0%	17.5%	3.80	0.284
Compliance	0.0%	32.5%	17.5%	35.0%	15.0%	5.00	0.172

Key: X1= Not implemented; X2= only some part has been implemented; X3= Implemented but has not been reviewed; X4= Implemented and reviewed on regular basis; X5= fully implemented and recognized as good for information security; χ^2 =chi-square.

Source: Researcher (2023)

From the findings, it was noted that compliance (50%) and server and network security (50%) were mostly implemented and reviewed on regular basis and recognized as good for information security. This was then followed by data security (35%); security awareness, training and education (35%); system software security (32%); physical and environmental security (30%).it was noted that Information security policy (15%) was the least implemented.

This implies that all technological, environmental and organization controls directly contribute to organization information security and that their individual implementations level affects the security posture of an organization(Ahmad & Mohammad, 2012).

4.2.5 Correlation Analysis

The analysis to determine the nature of relationship that existed between technological controls, Technological Controls, Organization Controls and Information Security Preparedness was computed using Pearson correlation which was tested at 0.01 Alpha Level against 1% level of significance. The findings are presented in a matrix Table 19.

Table 19

Correlation Analysis Matrix

		Information Security Preparedness
Technological Controls	Pearson Correlation	.623**
	Sig. (2-tailed)	.000
	N	40
Organization Controls	Pearson Correlation	.854**
	Sig. (2-tailed)	.000
	N	40
Environmental Controls	Pearson Correlation	.868**
	Sig. (2-tailed)	.000
	N	40

Source: Researcher (2023)

The study proved that there exist a positive and statistically significant relationship between technological controls and information security preparedness at 1% level of significance ($r= 0.623$; $p<0.01$). This implies that when measures relating to system software, security safeguarding, technological controls, network security and server security safeguarding are implemented in an organization, information security preparedness will be high.

Moreover, there exist a positive and statistically significant relationship between Organization Controls and information security preparedness at 1% level of significance ($r= 0.854$; $p<0.01$). This mean that when human resource security safeguarding measures, information security policy and awareness creation, training and education are implemented, it will improve on information security preparedness of the organization(Keung, 2014).

In addition, it was observed that there exist a positive and statistically significant relationship between environmental controls and information security preparedness at 1% level of significance ($r= 0.868$; $p<0.01$). This mean that when all relevant legislative, regulatory or contractual requirements related to security as well as physical and environmental security are implemented in the organization, it will also advance on their information security preparedness (Alkalbani et al., 2014).

4.2.6 Regression Analysis

In developing the model weights, multiple linear regression analysis was used to predict information security preparedness using the following equation:

$$Y=C+\beta_1X_1+ \beta_2X_2+ \beta_3X_3+ \varepsilon$$

The model summary of the analysis is presented in Table 20.

Table 20*Model Summary*

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.949 ^a	.900	.891	.21184
a. Predictors: (Constant), Environmental Controls, Technological Controls, Organization Controls				

Source: Researcher (2023)

The model indicates that 90% of the variation of information security preparedness is explained by Environmental Controls, Technological Controls and Organization Controls. This model leaves only 10% as unexplained variation which could be explained by factors outside the study variables. This corresponds with Otero (2014) study on basic indicators of information security in organization. Environmental controls, technological controls and organization controls directly affect an organization information security posture.

4.2.7 Model Significance

Model significance is tested using F –statistic shown in Table 21.

Table 21*F-Statistics*

Model		Sum of Df	Mean	F	Sig.	
		Squares	Square			
1	Regression	14.503	3	4.834	107.731	.000 ^b
	Residual	1.615	36	.045		
	Total	16.119	39			

a. Dependent Variable: Information Security Preparedness

b. Predictors: (Constant), Environmental Controls, Technological Controls, Organization Controls

Source: Researcher (2023)

It was established that at 0.05 Alpha Level, against 5% level of significance, the p value=0.000; $p < 0.05$ implies that the model predictors were significant in predicting information security preparedness.

4.2.8 Model Weights

The regression weights were computed as shown in Table 22.

Table 22

Coefficients^a

Model	Unstandardized Coefficients		Standardized Coefficients	T	Sig.	Collinearity Statistics	
	B	Std. Error	Beta			Tolerance	VIF
(Constant)	-.693	.214		-3.239	.003		
Technological Controls	.141	.072	.126	1.949	.059	.671	1.491
Organization Controls	.577	.096	.448	5.997	.000	.498	2.008
Environmental Controls	.569	.082	.506	6.965	.000	.528	1.894

a. Dependent Variable: Information Security Preparedness

Source: Researcher (2023)

The findings show that Organization Controls influences 57.7% of Information Security Preparedness and followed by Environmental Controls which influences 56.9%. Finally, Technological Controls influences 14.1% of Information Security Preparedness.

VIF statistics was used to measure the presence of multi-collinearity among predictor variables. When VIF is less than 10, then the predictor variables do not produce misleading beta coefficients

4.3 Derivation of Relevant Weights

The organization information security preparedness level was computed using linear regression modeling equation. The following equation was used to compute the necessary weights for determining organization information security preparedness level.

$$Y=C+\beta_1X_1+\beta_2X_2+\beta_3X_3+\varepsilon$$

Where

Y = Organization information security preparedness level (dependent variable)

β = Weights (regression coefficients)

X = Independent variable (information security controls)

C = Regression Constant

ε = standard error

The relevant weights for the model assigned for each assessment question;

$$\frac{1}{\text{Total Sum of possible scores}} = \text{Weight}$$

The percentage organization information security preparedness level was computed as;

$$\frac{\text{Total Sum of User Scores}}{\text{Total Sum of possible scores}} * 100 = Y$$

The regression formula was implemented in the system using the following code snippet;

```
SelectRound(100*((-0.48116+SUM(b.category_weight*a.user_score))^(0.48116+SUM(b.category_weight*5))),0) FROM tbl_self_assessment_results a INNER JOIN tbl_system_questions b ON a.qid=b.id WHERE a.user_id=$user_id"
```

Explanation:

The original regression formula was transformed in this format: **-0.48116+SUM (b.category_weight*a.user_score)** for coding.

Where;

- i. **-0.48116** is the sum of the constant value (-0.693) in the formula and the standard error value (0.21184) (as per the regression weights computed in table 22). The value of the constant computed is -0.693 while the value of the standard error computed is 0.241184. Therefore, for easy coding the summing of the two values was considered appropriate as the two values do not change.
- ii. **category_weight** is the regression coefficients in the formula for the Organization Controls (0.577000), Technological controls (0.141000), and Environmental Controls (0.569000). These weights were stored in the database on category_weight field for each question depending on the category for which they belong.
- iii. **user_score** is the score in a scale 1 to 5 for which the assessor checks for each question.

Therefore, the **SUM (b.category_weight*a.user_score)** is an SQL aggregate function that get multiplies the user score and the corresponding weight for each question (row) then sums to get the total user score. To compute the OISP for the user, then the new constant 0.48116 is added. This in itself is sufficient to compute OISP as an index.

To compute OISP as percentage, the sum above divided by maximum OISP index obtained when the user scores possible 5 in the Likert scale for all the questions then multiplied by 100. This is therefore depicted as **(-0.48116+SUM (b.category_weight*5))**.

It is worth noting that the OISP score obtained is for the session user **\$user_id**, that is the user who logs in.

4.4 Model Metrics

The organization information security preparedness level is determined by the getting the percentage score of the assessor. The higher the user score tending towards 100%, the higher organization information security preparedness level. The worst case scenario describes a case where the organization scores 1 in every question asked and the overall percentage score tends towards 0%.

4.4.1 Best Case Scenario

The best case scenario for the OISP model is where the organization is adequately prepared. This is realized when the user scores show that the department/ organization have fully implemented, reviewed and recognized that the existing information security controls are appropriate and updated. In that case, their information security preparedness level is 100%.

Best case scenario of OISP will be; $\frac{User\ Score}{Max\ Score} * 100 = 100\ %$

4.4.2 Worst Case Scenario

The worst case scenario is a scenario in which the assessment scores shows that the department/organization is poorly prepared. In this case the organizations information security preparedness level tends towards 0%. 0% is not possible because the user score are in a scale of 1 to 5, therefore the worst case scenario is achieved when a user score 1

in all questions and is calculated as follows; $\frac{User\ score}{Max\ Score} * 100 \rightarrow 0\ %$

4.4.3 Threshold Scores

According to OISP model, the threshold scores in a scale of 1 to 5 is are pegged at 4 and 3. At 4 the assessor agrees that a given information security practice has been fully implemented and is regularly reviewed showing that the department or organization is adequately prepared. The highest score of 5 denotes that the organization\department acknowledges that their information security practices are appropriate to their organization\department in curbing information security threats. Scores pegged at 3 shows that the organization or the department is averagely prepared and have implanted the said controls and are yet to review and updated the controls. Scores below the threshold score 3 means that the preparedness level is poor and that the department\organization is at a vulnerable position. Therefore, such scenario calls for action by the organization to minimize the risk. Recommendations for best practices are pecked on the threshold scores.

4.5 Model Implementation

Implementation is the executing, or practicing a plan, a method, a design, an idea, model, specification, standard or policy for doing something(Rouse, 2019). In an information system context, implementation involves analyzing requirements, design, coding, running, testing, integrating, user training, and making necessary changes. This section provides a detailed description of how the model was designed, implemented and evaluated as a web based model. It therefore, fulfils objective three of the study. This study used rapid prototyping approach to implement the model as discussed in chapter three section 3.8.

4.5.1 Model Objectives

The main objective of the OISP model is to provide an effective way in which key information security personnel in a county government can individually assess their organization preparedness level in regards to information security. The model should be able to highlight the information security practices that require reviewing and update so as to appropriately protect e-governance systems hence improve citizen's trust in e-governance. Furthermore, the model should provide a detailed report on assessments done. The model is to be used as a platform for conducting information security assessments by county governments so that they can maintain a sound security level by updating their information security practices according to the recommendations suggested by model.

4.5.2 Model Requirements Specifications

Requirement specifications are a detailed description of the functions and capabilities a system should exhibit and constraints it should operate within. According to Sommerville (2010), requirements specifications are grouped into two groups: functional and non-functional (business) requirements.

4.5.2.1 Functional Requirements

Sommerville (2010) defines system functional requirements as statements describing services the system should provide. They define how a system should operate in particular situations and react to particular inputs (Sommerville, 2010). The following functional requirements were identified for the model:

- i. The OISP platform should provide a functional web-based interface for information security personnel to assess their security preparedness level.

- ii. The model is expected to provide information security personnel with appropriate recommendation for improving their security preparedness level through a responsive and simple graphical interface.
- iii. The model is expected to provide the Chief information security officer with a detailed report on overall preparedness level of the county government through a simple graphical interface.

4.5.2.2 Business Requirements

These are requirements that relate to the fundamental business of an organization. Business (non-functional) requirements represent the constraints on the system and its functionalities; performance constraints; compliance with standards, (Sommerville, 2010). In information security, any system adopted or implemented should ensure the confidentiality, integrity and availability of information. The study identified the following non-functional requirements.

- i. The model should comply with the government of Kenya information security standards outlined in the GEA standard and guidelines for information security management outlined in the international best practices.
- ii. The model should seamlessly integrate with existing information security management system.
- iii. The model should be scalable.

4.5.3 Model Overview

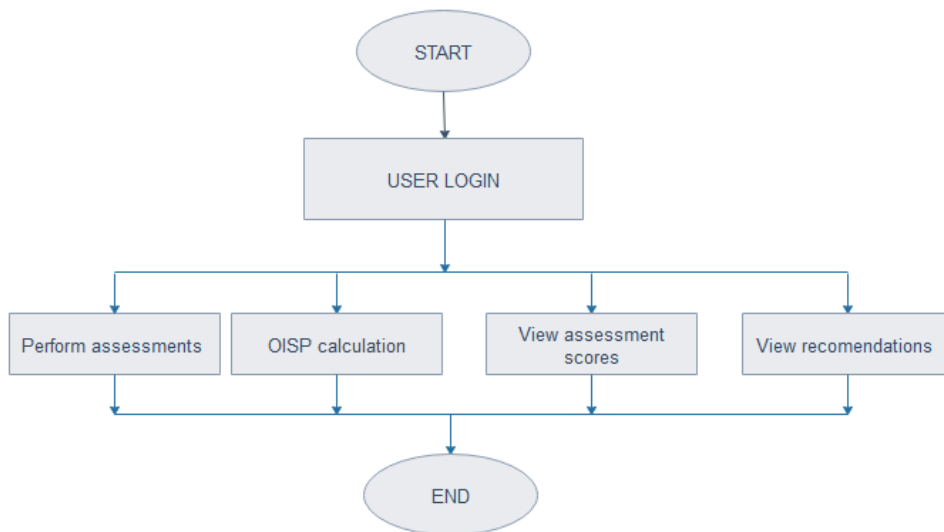
The model was developed using PHP as server side scripting language, MySQL as a database engine, CSS3 for styling and JQuery for interactive functions. Security was enforced in the web based model to ensure that all users would be authenticated before conducting any assessment or accessing any other system functionality. All users are

required to login providing their unique log in details as assigned by the Chief information security officer. The chief information security officer registers all users according to their roles and responsibilities in information security and assign them assessment questions according to their responsibilities.

The flowchart in figure 13 below represents the overall functionality of the OISP platform.

Figure 16

OISP System Flowchart



Source: Researcher (2023)

4.5.4 System Contributors

During the implementation of the OISP model a number of partakers were involved, who include; system users and administrators, domain name registrar, and web hosting service provider.

- i. **System users and administrators:** Users of OISP system are those who login successfully and are able to carry out assessments tasks within the OISP platform.

They include key information security personnel in county governments that are responsible for information security management. The administrator position was reserved for chief information security officer who is the lead player in management of security risks in governments and organizations. Unlike the other system users, the CISO is able to register other personnel, and also view the overall scores of information security preparedness levels from all other user assessments. Furthermore, the CISOs are able assign roles responsibilities to other personnel involved in information security management and update assessment checklists in case the current checklist changes.

- ii. **Domain registrars:** Domain name registrar is responsible for registration and reservation of the domain name for the OISP platform on the internet.
- iii. **Web host:** These are web hosting service providers who ensure that there is assured availability of the OISP system online by providing hosting space on their servers as well as services and technologies required for the webpages to be displayed on the Internet. The web server allows communication between users and the OISP platform.

4.5.5 OISP System Architecture

This section describes the OISP abstract model that defines the structure, behavior and views of the system. It presents the modules that make up the OISP system, the entity relationship diagram of the OISP model and the logical design of the OISP system.

4.5.5.1 OISP Modules

The OISP model has eight modules that work together to achieve the OISP system functionality.

- a) **User login and authentication module:** This module ensures that only the registered users who have permission to access the functionality are allowed access the system while others are denied access. The registered users are required to provide the email and password matching the ones assigned by the system administrator who is the CISO so as be granted access.
- b) **User Session Handling Module:** This module manages user sessions by creating a session when user logs into the system, track all the user activities when the session is on, and destroys the session when the user logs out of the system.
- c) **Information security Assessment module:** This session pulls the assessment questions from the database and present it on a Likert scale layout. The user goes through the questions and checks the appropriate answer depending on the level of implementation of their organization's information security practices. After all the questions have been duly filled the user submits it.
- d) **Reports module:** This module presents the results of the submitted assessment to the user in a graphical display. The user can also download the assessment results and recommendations in the form of portable document format (pdf). Additionally, there is a separate admin report module that is only accessible to the CISO, where the CISO can view all other users' assessment reports and the overall organization preparedness level.
- e) **Core application logic:** This module contains logic that handles user requests by receiving, processes, and responding to them. Additionally, this module allows inputs to the database, performs arithmetic computations of the information security preparedness level.
- f) **Settings module:** This module is only accessible to the system admin. It enables the CISO to register other system users by assigning them roles according to their

responsibilities in information security management and also add new roles. In addition, it allows the CISO to add and modify the assessment questions depending on the adopted practices of the organization.

g) **Database:** The OISP model maintains a database that contains four main tables for storing information.

The OISP database contains four tables for storing different types of information;

1. **User information table:** id, user_role_id, first_name, last_name, email, password, active

Field	Type	Null	Key	Default	Extra
<input type="checkbox"/> id	int(11)	7B NO	PRI	(NULL)	OK auto_increment
<input type="checkbox"/> user_role_id	int(11)	7B YES		(NULL)	OK
<input type="checkbox"/> first_name	varchar(255)	12B YES		(NULL)	OK
<input type="checkbox"/> last_name	varchar(255)	12B YES		(NULL)	OK
<input type="checkbox"/> email	varchar(255)	12B YES		(NULL)	OK
<input type="checkbox"/> password	varchar(255)	12B YES		(NULL)	OK
<input type="checkbox"/> active	tinyint(1)	10B YES		(NULL)	OK

2. **User role information table:** id, user_role

Field	Type	Null	Key	Default	Extra
<input type="checkbox"/> id	int(11)	7B NO	PRI	(NULL)	OK auto_increment
<input type="checkbox"/> user_role	varchar(100)	12B YES		(NULL)	OK

3. **System Questions information table:** id, question, category, main_category, recommendation, category_weight, threshold, ciso, sysadmin, hr, netadmin, others

Field	Type	Null	Key	Default	Extra
<input type="checkbox"/> id	int(11)	7B NO	PRI	(NULL)	OK auto_increment
<input type="checkbox"/> question	varchar(255)	12B YES		(NULL)	OK
<input type="checkbox"/> category	varchar(255)	12B YES		(NULL)	OK
<input type="checkbox"/> main_category	varchar(255)	12B YES		(NULL)	OK
<input type="checkbox"/> ciso	tinyint(1)	10B YES		0	1B
<input type="checkbox"/> sysadmin	tinyint(1)	10B YES		0	1B
<input type="checkbox"/> hr	tinyint(1)	10B YES		0	1B
<input type="checkbox"/> netadmin	tinyint(1)	10B YES		0	1B
<input type="checkbox"/> others	tinyint(1)	10B YES		0	1B
<input type="checkbox"/> category_weight	double(12,6)	12B YES		(NULL)	OK
<input type="checkbox"/> recommendation	varchar(255)	12B YES		(NULL)	OK
<input type="checkbox"/> threshold	double(12,2)	12B YES		(NULL)	OK

4. **Self-assessment information table:** id, role_id, user_score, asst_date, qid, user_id.

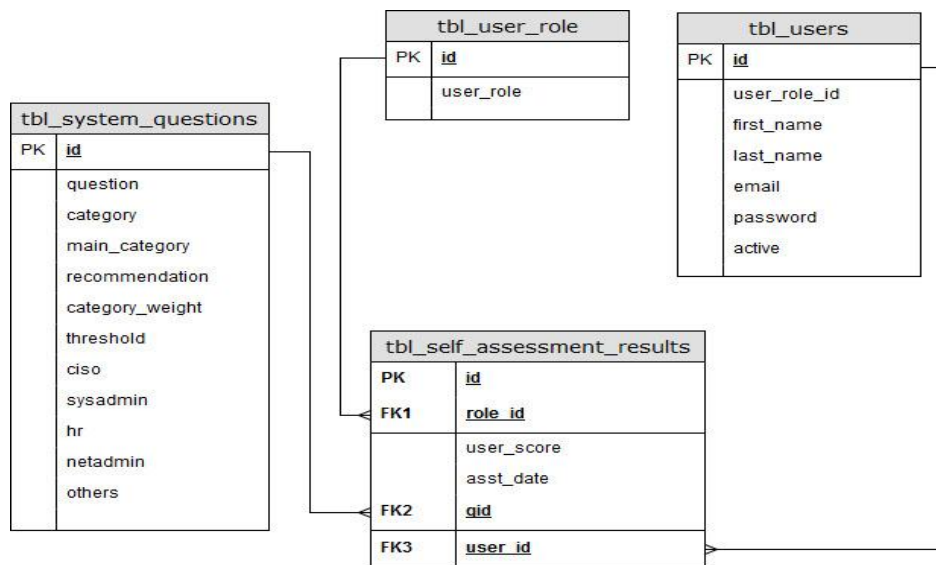
Field	Type	Null	Key	Default	Extra
<input type="checkbox"/> id	int(11)	7B NO	PRI	(NULL)	OK auto_increment
<input type="checkbox"/> qid	int(11)	7B NO		(NULL)	OK
<input type="checkbox"/> user_id	int(11)	7B NO		(NULL)	OK
<input type="checkbox"/> role_id	int(11)	7B NO		(NULL)	OK
<input type="checkbox"/> user_score	int(11)	7B NO		(NULL)	OK
<input type="checkbox"/> asst_date	timestamp	9B NO		CURRENT_TIMESTAMP	17B

4.5.5.2 Entity Relationship Diagram

The entity relationship diagram for the OISP system is presented in figure 17 below.

Figure 17

Entity Relationship Diagram



Source: Researcher (2023)

4.5.5.3 OISP Logical and Physical Design

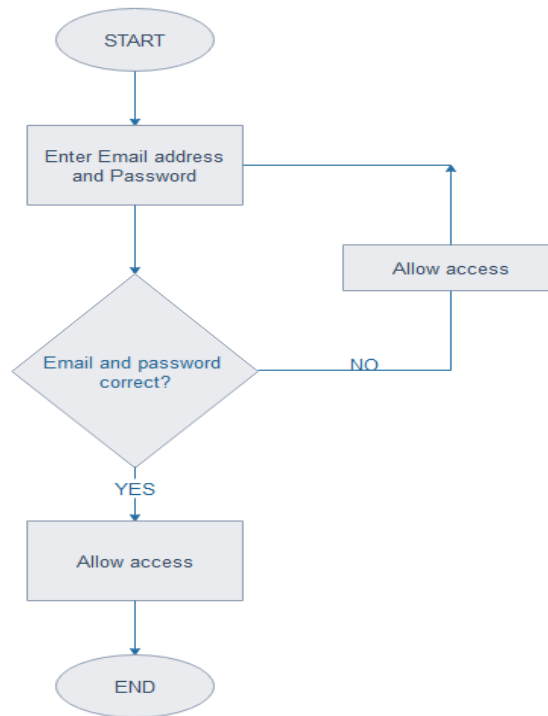
The logical design of a system refers to an abstract representation of the data flows, inputs and outputs of the system. The physical design is a graphical representation of a system showing the system's internal and external entities, and the flows of data into and out of these entities. This section presents the logical design of the OISP system using flowcharts and user interface design of the implemented OISP modules

4.5.5.3.1 User Login and Authentication Module

This module manages logins and sessions on users. It allows registered users to access system functionality by referring to users' database. If the user is not registered it denies them access and prompts them to provide correct usernames, passwords or register. Figure 18 below shows a flowchart representing the logic of the login system while Figure 19 presents a graphical user interface of the login component.

Figure 18

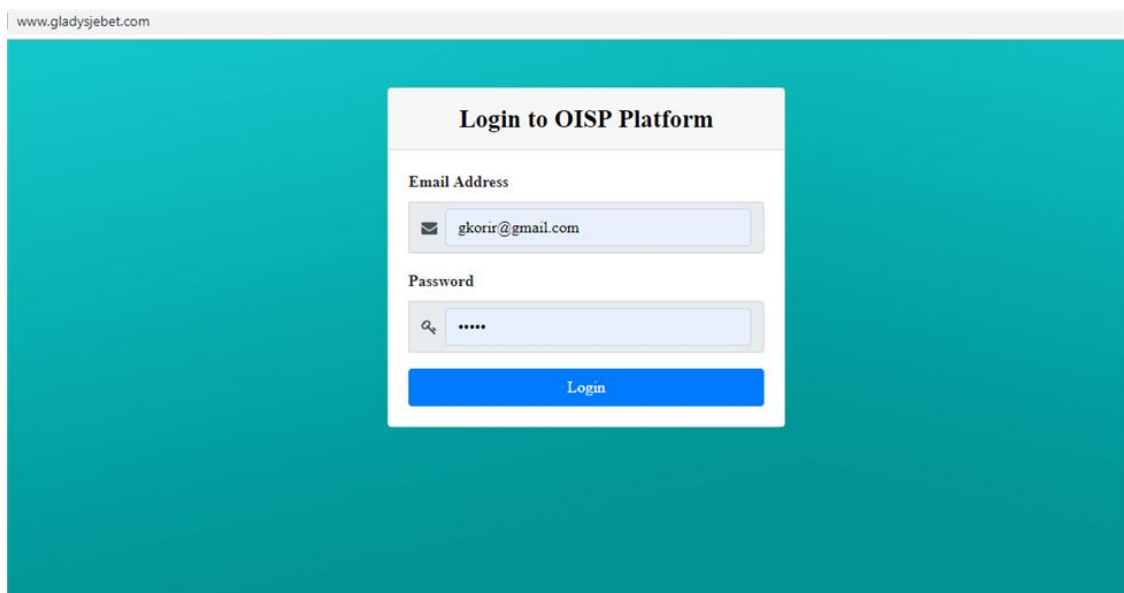
Login Flowchart



Source: Researcher (2023)

Figure 19

OISP Login GUI



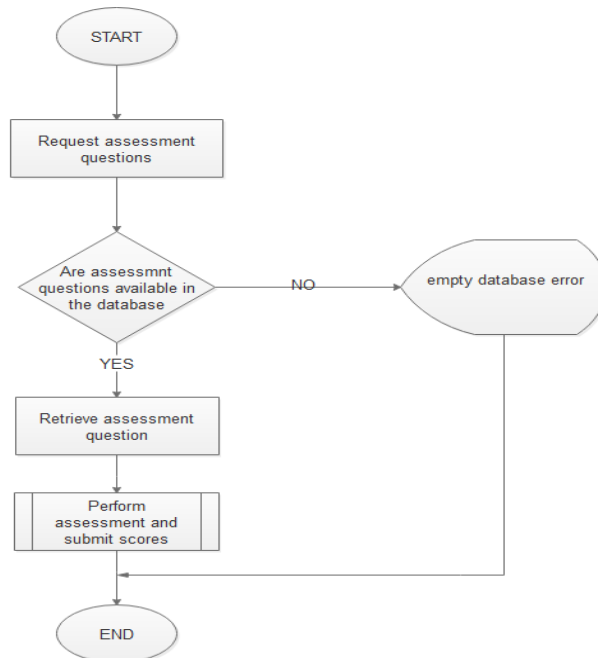
Source: Researcher (2023)

4.5.5.3.2 Information Security Assessment Module

Once a user has logged in, the user can perform assessment using the information security self-assessment module. This module allows the user to perform self-assessment for their organization/department by answering every assessment question in a Likert scale of 1 to 5. This module retrieves the questions from the database and presents it to the user in a Likert scale layout. Duly filled assessment form can be submitted to the database from where the information security preparedness level will be computed. The Figure 20 below shows a flowchart presentation of the assessment logic whereas Figure 21 is the presentation of the graphical user interface of the information security assessment module.

Figure 20

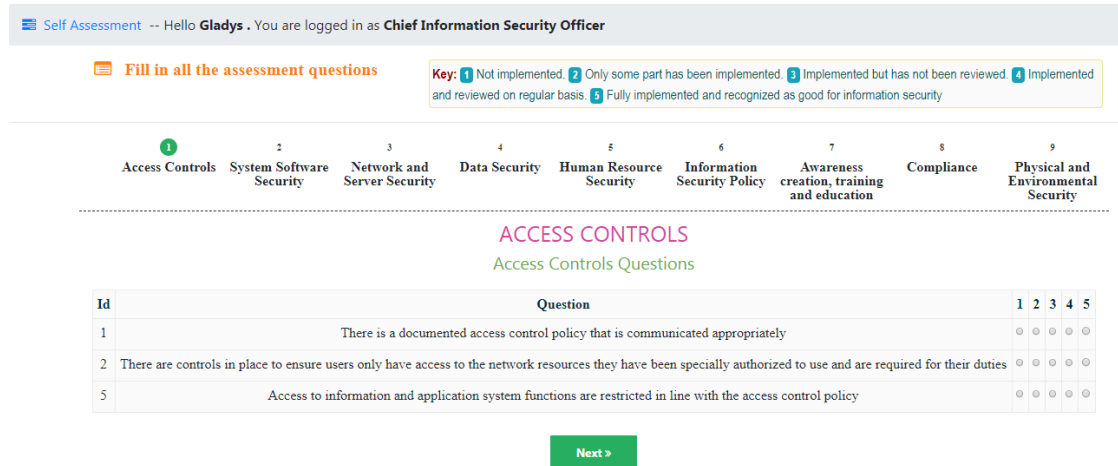
Self-Assessment Module



Source: Researcher (2023)

Figure 21

Self-assessment GUI



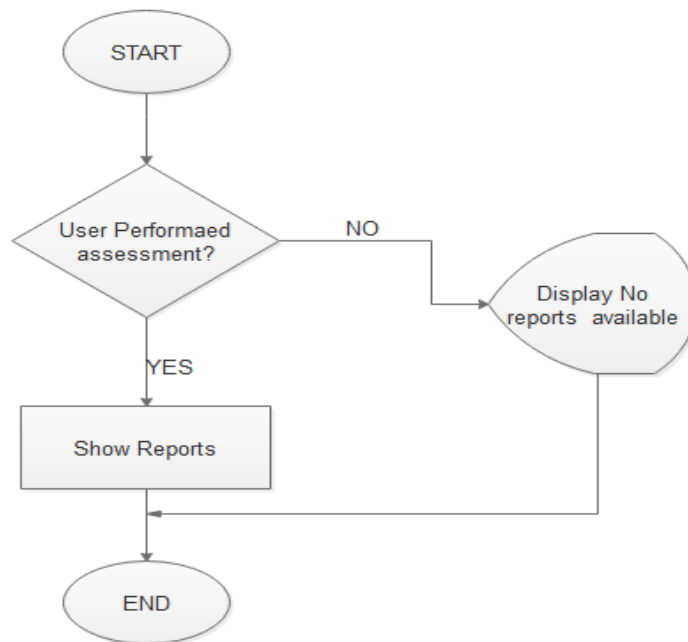
Source: Researcher (2023)

4.5.5.3.3 Reports Module

This component of the OISP model allows the user to read back their assessment scores for all the assessment questions submitted. It also allows the user to download the scores in a portable document format that can be printed. The reports module is further divided to user scores, recommendations and admin reports. Figure 22 illustrate the flowchart representation for retrieving the reports.

Figure 22

Assessment Report Flowchart



Source: Researcher (2023)

a) User Scores Reports

The Figure 23 below shows the graphical user interface for the user scores reports.

Figure 23

User Score Report GUI

Your Self-Assessment Scores Per Question Average: 2.759 /5.000

Question ID	Question	Your Average Score (1-5)
1	There is a documented access control policy that is communicated appropriately	2.0000
2	There are controls in place to ensure users only have access to the network resources they have been specially authorized to use and are required for their duties	2.5000
5	Access to information and application system functions are restricted in line with the access control policy	2.0000
6	There are established procedures which list all requirements with regard to outsourcing any county Information Systems service or activities.	2.0000
7	There are anti-spyware, anti-phishing and cleanup software solutions to detect, prevent and remove any spyware threats, phishing attacks and trashed files regularly.	2.5000
8	There is a rollback software to keep track and record any changes made to the computers and allow the system to be restored to its original state from any chosen point in time.	3.5000
13	There is authentication systems to prevent unauthorized access to the countys server.	3.0000
14	There is routine backup for the data, safe storage of hard copy of server hardware specifications, installation information, installation software and passwords at an offsite location.	3.5000
15	The server is placed in a secure location, such as in a lockable cage, a locked room and place it with environmental controls.	3.0000
16	There are data classification, retention and destruction procedures for handling county data, media or materials that contain county sensitive information.	3.0000
18	There are policies on sharing, storing and transmitting of county data via ISPs, external networks or contractors systems.	4.0000
19	Use of cryptography techniques, hardware & software tokens and single sign on systems to control data access to the county internal and remote computer systems	3.0000

Source: Researcher (2023)

b) Recommendation Reports

The figure 24 below shows the graphical user interface for the recommendation reports

Figure 24

Recommendation Reports GUI

Recommendations Report-- Hello Gladys . You are logged in as Chief Information Security Officer

Your Recommendations for Best Practice **16 Recommendations**

Question ID	Your Average Score (1-5)	Recommendation
1	1.0000	You should have a documented access control policy that is communicated appropriately
2	1.0000	Controls should be in place to ensure users only have access to the network resources they have been specially authorized to use and are required for their duties
5	1.0000	Access to information and application system functions are restricted in line with the access control policy
6	1.0000	There are established procedures which list all requirements with regard to outsourcing any county Information Systems service or activities.
7	2.0000	There are anti-spyware, anti-phishing and cleanup software solutions to detect, prevent and remove any spyware threats, phishing attacks and trashed files regularly.
20	1.0000	Vital Countys business information or records are regularly backed up and stored in a different site.
27	1.0000	There are policies on protection of county assets to protect your countys hardware, software, data and people.
30	2.0000	Procedures for update and review existing information security policies
33	2.0000	Information security awareness trainings is mandatory to all staff and patrons at various levels.
34	2.0000	There are balanced set of key performance indicators (KPIs) and metrics used to provide the real insight into the effectiveness of security awareness programs.
37	1.0000	All the records within the county are protected from loss, destruction, falsification and unauthorized access or release in accordance with legislative, regulatory, contractual and business requirements

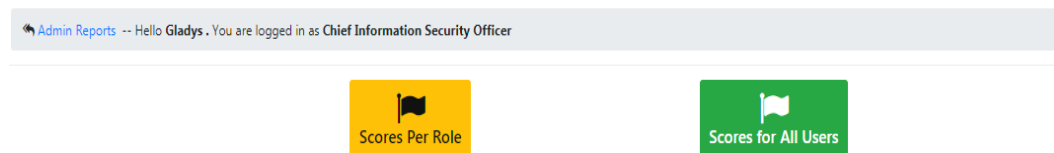
Source: Researcher (2023)

c) Admin Reports

The figure 25 below shows the graphical user interface for the administrator’s reports

Figure 25

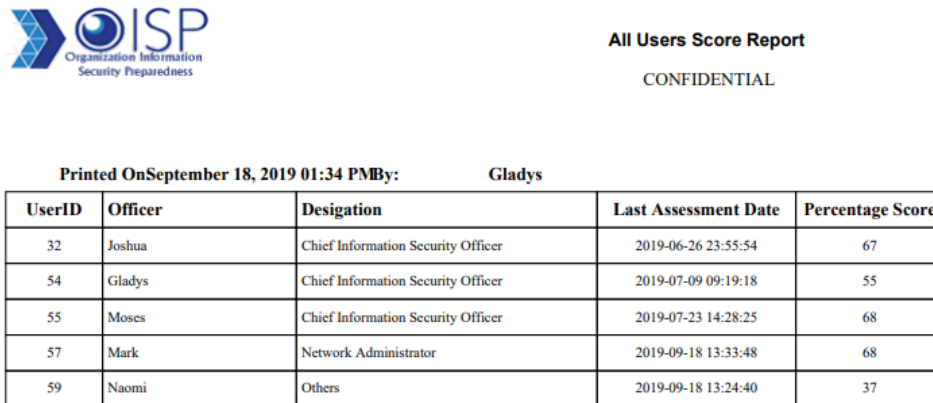
Admin Report GUI



Source: Researcher (2023)

Figure 26

OISP Users Score Report GUI



UserID	Officer	Desigation	Last Assessment Date	Percentage Score
32	Joshua	Chief Information Security Officer	2019-06-26 23:55:54	67
54	Gladys	Chief Information Security Officer	2019-07-09 09:19:18	55
55	Moses	Chief Information Security Officer	2019-07-23 14:28:25	68
57	Mark	Network Administrator	2019-09-18 13:33:48	68
59	Naomi	Others	2019-09-18 13:24:40	37

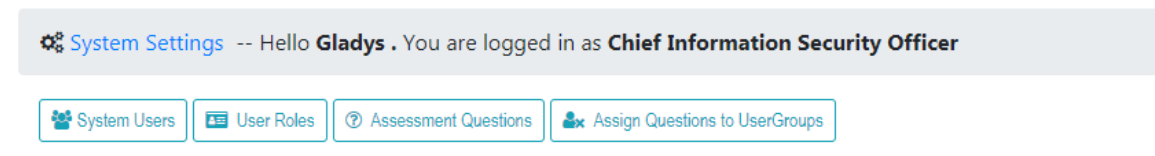
Source: Researcher (2023)

4.5.5.3.4 Setting Module

The setting module enables the CISO to register other system users by assigning them roles according to their responsibilities in information security management and also add new roles. In addition, it allows the CISO to add and modify the assessment questions depending on the adopted practices of the organization.

Figure 27

Setting GUI



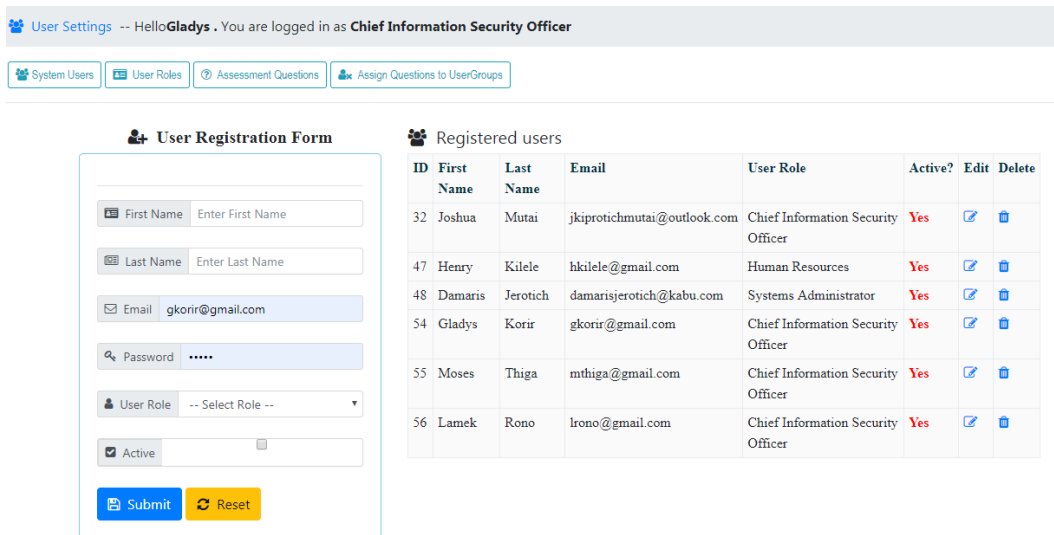
Source: Researcher (2023)

a) System Users' Registration

This sub-module allows the CISO to register other users to the system according to the roles and responsibility in information security management. Figure 28 below shows the graphical user interface for this sub-module.

Figure 28

User Registration GUI



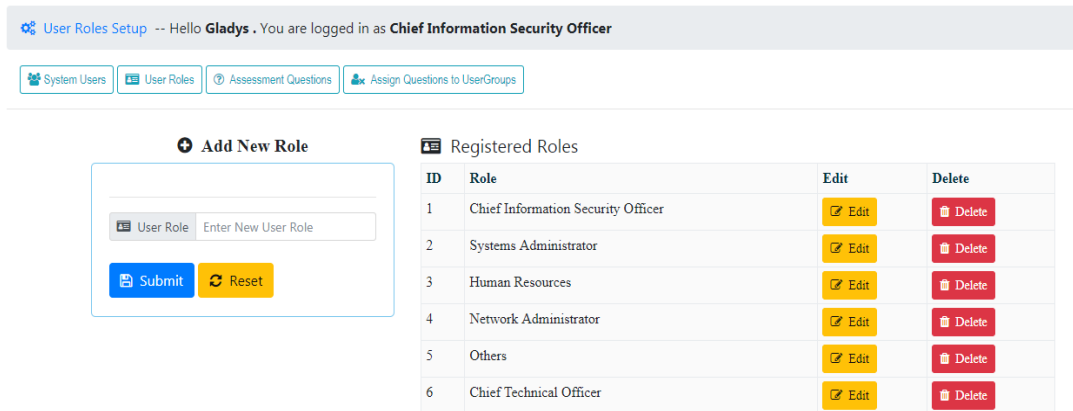
Source: Researcher (2023)

b) User roles

This sub-module allows the CISO to add new role to the system according to their need in information security management. Figure 29 below shows the graphical user interface for this sub-module.

Figure 29

New Role Registration GUI



Source: Researcher (2023)

c) Assessment questions

This sub-module allows the CISO to add more assessment questions to the information security assessment questions checklist. Figure 30 and 31 below shows the graphical user interface for this sub-module.

Figure 30

All Questions Lists GUI

Id	Category	Main Category	Question	Edit	Delete
1	Access Controls	Technological controls	There is a documented access control policy that is communicated appropriately	Edit	Delete
2	Access Controls	Technological controls	There are controls in place to ensure users only have access to the network resources they have been specially authorized to use and are required for their duties	Edit	Delete
3	Access Controls	Technological controls	There is formal user access registration process and a formal user access provisioning process for assigning access rights for all user types and services	Edit	Delete
4	Access Controls	Technological controls	There is a process to ensure user access rights are removed on termination of employment or contract, or adjusted upon change of role	Edit	Delete

Source: Researcher (2023)

Figure 31

Add New Assessment Question GUI

The screenshot displays the 'Add New Assessment Question' GUI. At the top, there is a navigation bar with four tabs: 'System Users', 'User Roles', 'Assessment Questions', and 'Assign Questions to UserGroups'. Below the navigation bar, the main content area is titled 'Add New Assessment Question' and includes a 'Back to List' button. The form itself contains the following elements:

- A 'Question' text input field with the placeholder text 'Enter New Assessment Question'.
- A 'Category' dropdown menu with the placeholder text '-- Select Category --'.
- A 'Main Category' dropdown menu with the placeholder text '-- Select Main Category --'.
- A 'Recommendation' text input field with the placeholder text 'Enter Recommendation'.
- At the bottom of the form, there are two buttons: a blue 'Submit' button and a yellow 'Reset' button.

Source: Researcher (2023)

d) Assign questions to user groups

This sub-module allows the CISO to assign assessment questions to users with different roles in information security management. Figure 32 below shows the graphical user interface for this sub-module.

Figure 32

Assigning Questions GUI

		Grant/Revoke Permissions Grant All Revoke All					
Id	Category	Question	CISO	System Admin	Human Resource	Network Admin	Others
			<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1	Access Controls	There is a documented access control policy that is communicated appropriately	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	Access Controls	There are controls in place to ensure users only have access to the network resources they have been specially authorized to use and are required for their duties	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	Access Controls	There is formal user access registration process and a formal user access provisioning process for assigning access rights for all user types and services	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4	Access Controls	There is a process to ensure user access rights are removed on termination of employment or contract, or adjusted upon change of role	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5	Access Controls	Access to information and application system functions are restricted in line with the access control policy	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6	System Software Security	There are established procedures which list all requirements with regard to outsourcing any county Information Systems service or activities.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7	System Software Security	There are anti?spyware, anti-phishing and cleanup software solutions to detect, prevent and remove any spyware threats, phishing attacks and trashed files regularly.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8	System Software Security	There is a rollback software to keep track and record any changes made to the computers and allow the system to be restored to its original state from any chosen point in time.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

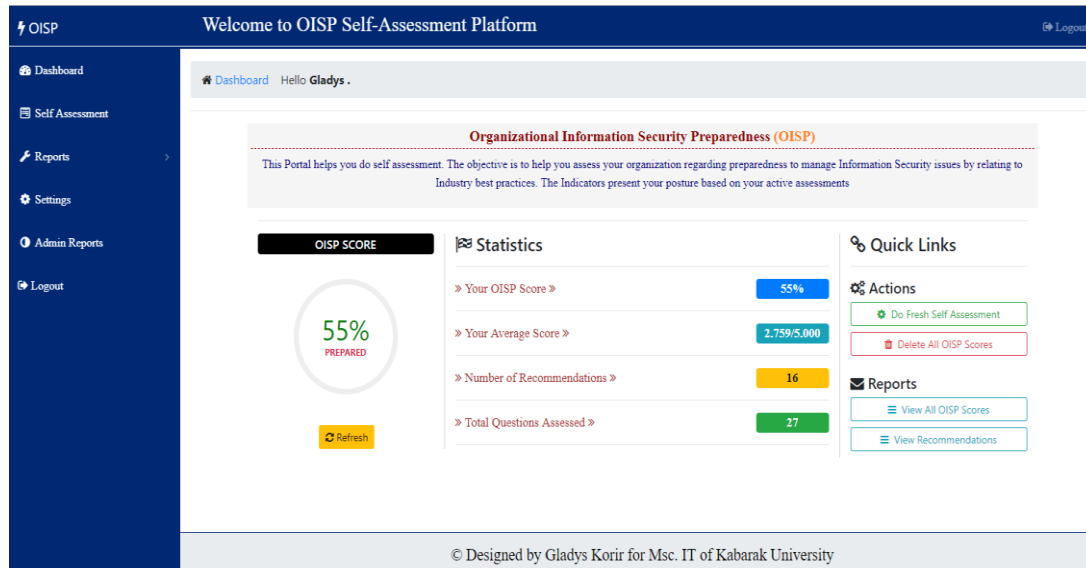
*Source:*Researcher (2023)

4.5.5.4 OISP System Interface

The OISP system has a responsive user interface that once a user has successfully logged in to the system, one can easily interact with the system components and navigate the different modules. The Figure 33 presents a graphical user interface layout of home display component.

Figure 33

OISP Dashboard



Source: Researcher (2023)

4.5.6 Proof of Concept

As a proof of concept, the OISP platform was developed using PHP server side scripting language for system logic controllers. Front end scripting was done using JQuery library to enhance front end responsiveness to the platform while styling was done using Cascading style sheets version 3 (CSS3). Visio studio code and notepad++ program editors were used to write and test code. Apache web server was used to run the application locally and MySQL was used as backend database engine. The system was deployed online and can be accessed using the following URL; www.gladysjebet.com.

4.6 Model Evaluation

In order to determine how effective, the OISP model was in achieving its preset objectives, an evaluation was undertaken guided by a goal-based evaluation approach which determines the extent at which a system is achieving the pre-set objectives. Each

functionality of the OISP model was tested with regards to its objectives as presented in the Table 23 below;

Table 23

Goal-Based Evaluation for the OISP System

Objective	Evaluation Results
1. User login and Authentication: The system was expected prompt user to provide login credentials before being allowed to access the system components.	<ul style="list-style-type: none"> i. The system prompted user for login credentials and matches with the ones stored in the database. ii. The system allowed access to users who successfully provided username or email and password that matches those stored in the database.
2. Information security assessment and submission: The system was supposed to retrieve assessment questions from the database and present to the user in a Likert scale layout. It was also to allow the user to submit duly filed assessment form to the database	<ul style="list-style-type: none"> i. The system was able to retrieve assessment questions and from the database and present them in an easy-to-use Likert scale format for the user. ii. It also allowed the user to submit score from a duly filled assessment form into the database.
3. OISP calculation: The system was expected to compute the preparedness level as per submitted user scores and present the results to the user in percentage	<ul style="list-style-type: none"> i. The system was able to read the user scores from the database and determine the preparedness level as per the user scores. ii. It provided the preparedness level as a percentage.
4 Reports and recommendations: The system was expected to retrieve reports on assessment scores and recommendations and allow the user to download the output into a portable and printable document format.	<ul style="list-style-type: none"> i. The system was able to retrieve the scores as well as recommendations from the database and present them to the user ii. It was also able to allow the user to download the output into a portable document format that can be printed.
5 Registration of new users and addition of new assessment questions: The system was supposed to allow registration of new users as per their roles and responsibilities in information security management. Also allow assignment of assessment questions as per their roles and responsibilities.	<ul style="list-style-type: none"> i. The system was able to allow registration of new users as per their roles and responsibilities in information security. ii. It also allowed assigning of different assessment questions to the new users as per their roles and responsibilities in information security management.

Source: Researcher (2023)

The OISP model was designed, implemented and deployed online then users were allowed to register, login and perform their independent assessment using the system. It was noted that the system had captured the details of the users, encrypted their passwords using MD5 hash function. The records of user scores were also stored in the database successfully with timestamps attached to each assessment row. In addition, reports of OISP computation for all the users that logged in and submitted their scores could be accessed by the chief information security officer.

4.6.1 Model Validity

Validity of a tool or an instrument determines to what extent do the instrument measures what it was designed to measure. To test the validity of the OISP model, a validation exercise was conducted. Validation was done as part of the evaluation process of the OISP in order to determine whether the model was capable of measuring organization information security preparedness level effectively. Ten study participants were selected randomly from the study population target to undertake the validation exercise. Each participant was guided on how to validate the model. The participants were then given access credentials to the model according to their roles and given a reporting template (Appendix II) to provide their feedback concerning model validity. The participants were expected to evaluate each module of the model against the preset objectives in a scale of 1 to 3, where 1 means the module is not effective, 2 partially effective, and 3 effective.

The analysis of the validity are presented in Table 24 below.

Table 24*Validity Analysis*

Module	Objective	Percentage effectiveness	Remarks
User login and authentication	The model should prompt user to provide login credentials before being allowed to access the system components and only allow users who successfully provided username or email and password that matches those stored in the database.	100%	This module works effectively
User session handling	The model should create sessions when users logs into the model, track all the user activities when the session is on, and destroys the session when the user logs out of the system.	100%	This module works effectively
Information security assessment	The model should retrieve assessment questions from the database and present to the user in a Likert scale layout and also allow the user to submit duly filed assessment form to the database	100%	This module works effectively
Reports module	The model should retrieve reports on assessment scores and recommendations and allow the user to view or download the results. Additionally, the administrator who is the CISO should be able to view all other users' assessment reports and the overall organization preparedness level.	100%	This module works effectively
Settings	This module should only be accessible to the user with administrator privileges. It should enable them to register other system users by assigning them roles according to their responsibilities in information security management and also add new roles. In addition, they should be able to add and modify the assessment questions depending on the adopted practices of the organization.	100%	This module works effectively
OISP calculation	The model should compute the preparedness level as per submitted user scores and present the results to the user in percentage.	100%	This module works effectively

Source: Researcher (2023)

The validity analysis showed that the OISP was effective in determining organization information security preparedness level and performing the predefined objectives.

4.7 Scalability

In case of additional users and security control measures, the OISP model has the functionality to allow addition of more users and security control measures questions. Also the OISP assessment questions can be customized by the chief information security officer so as to match their existing information security practices.

Although the OISP system design was scoped to the county governments in Kenya and based on nine areas of information security controls, it has the potential of being scaled to include other information security controls and applied to organizations other than county governments and countries.

CHAPTER FIVE

SUMMARY, CONCLUSIONS AND RECOMMENDATIONS

5.1 Introduction

This chapter presents the thesis summary, the conclusion on the study, how each objective of the study was achieved and finally provide the recommendations.

5.2 Summary of the Major Findings

As Kenya's ICT grows, e-governance has become the formal way of providing improved public services to Kenyan citizens. Since 2004, when the government of Kenya approved e-government strategy for public service delivery, the government of Kenya have initiated several e-governance systems with the aim of enhancing efficiency, transparency and democracy in public administration. These systems have eased the burden of many citizens of accessing government services and also have improved government operation. However, e-government implementation has encountered several challenges which include cyber-attacks and information security breaches. These challenges have resulted in citizens' mistrust in e-governance systems to secure their critical information.

In Kenya, information security in e-governance have been addressed using different approaches but still appear to be weak. The government have invested heavily in technical and non-technical information security practices. However, these practices lack realistic strategies that are focused at improving organizational information security measures which have caused governments to be reluctant in reviewing and updating their information security measures towards counteracting the dynamic nature of information security threats.

To improve overall information security, governments and organizations must assess their information security practices regularly so as to determine their security capability and thus review and update their information security practices to satisfy their specific security requirements and to overcome the challenge of the dynamic nature of information security threats (Otero, 2014). Since governments are continuing to be the major targets for cyber criminals, new and innovative ways must be created to solve every problem that affect the security of e-governance (Karokola, 2012). A web-based model for determining organization information security preparedness level proposed in this study, not only addresses the problem above, but also provides an effective and efficient way of assessing information security capabilities by key personnel in different departments dealing with e-governance security in governments. Routine information security assessment will help governments stay proactive with the right information security control measures in place so as to quickly adapt to the evolving nature of information security threats.

This study adopted design research science methodology so as to realize the research objectives and satisfactorily address the research questions. Rapid prototyping was used in the development and designing of the model. The study was carried out in Uasin Gishu county government. The research target population included the county executive members, ICT staff, chief information security officers in the counties and information systems users and custodians within the county governments. Questionnaires were used as the data collection instrument. Data analysis was done using both descriptive and inferential statistics. The OISP model was developed as a web-based model for assessing information security preparedness level in governments. The designed OISP solution was able to effectively assess information security control measures put in place to safeguard e-governance systems in county governments.

5.3 Conclusion

The alarming facts related to e-governance success in Kenya, point to existent inadequacies and inefficiencies in regards to information security practices employed to secure e-governance systems. An extensive survey of literature and existing information security practices adopted by the governments, revealed that the Kenyan government have invested heavily in technical and no-technical measures to protect and preserve their information systems, however have failed to regularly review and update their practices so as to be able to match with the evolving nature of information security threats. Analysis of the existing information security assessment methodologies showed that there was no precise methodology that has been developed to assess information security in Kenya.

The premise upon which this research was based on is the inadequacy of information security assessment methods used by information security personnel in county governments in Kenya to assess and review their information security practices. The proposed model is an organization wide assessment platform where key information security personnel in governments individually assess their department/organization information security practices to determine their level of preparedness and their capability to reduce evolving information security risks.

The proposed model addresses the research gap identified in chapter two of this study in the following ways; it provides a simplified, reliable and efficient way in which county governments in Kenya can determine their information security preparedness level at any time. It automates the processes of information security assessments in governments. It assesses all aspects of information security practices in an organization ranging from

organizational controls, technological controls and environmental controls and also provide a way for addition or removal of new or obsolete information security practices.

This model is aimed at strengthening of information security practices adopted by governments so that there is better management of information security risks.

Conclusions related to specific objectives are presented in the next section

5.3.1 Fundamental Information Security Controls that can be used to Determine OISP Level in E-governance

From recognized theories, the study established that the key information security controls required to achieve sound information security level in any organization are technological, organizational and environmental controls. Most international best practices for information security management recommended controls overlap in those categories. The proposed model therefore, considered nine information security controls suggested by international best practices categorized under the three TOE dimensions of information security implementation. Technological controls; Access controls, Network and server security controls, System software security controls, Data security controls. Organizational controls; Human resource security controls, Security awareness, training and education, Information security policies. Environmental controls; Compliance, Physical and environmental security. These controls contribute to realization of an ideal information security in county governments in Kenya.

5.3.2 OISP Model Development

To develop the OISP system, a Design Research Science methodology and rapid prototyping were used. Design research science was important in identifying the specific objectives of the model while rapid prototyping guided the researcher in designing and developing the model within the shortest time possible. Development of the model

involved analyzing of the model requirements, designing, coding, running, testing, integrating, user training, and making of the necessary changes.

5.3.3 OISP Model Implementation

The model for determining OISP was implemented as a web based application using PHP as a server-side language, JQuery for frontend interactions, and MySQL as a database engine. The model has a database for storing assessment questions information, assessment scores information and system users' information. The model relies on the assessment information stored in the database to determine information security preparedness level of the assessor. The model provides the user with their level of preparedness and recommendation necessary to improve their information security practices.

5.3.4 OISP Model Evaluation

In order to determine how effective the OISP system was in achieving its preset objectives, an evaluation was undertaken guided by a goal-based evaluation approach, which determines the extent at which a system is achieving the pre-set objectives. Furthermore a validity test was conducted to test the validity of the model. Each functionality of the OISP system was tested with regards to its objectives.

5.4 Recommendations

5.4.1 Policy Recommendation

The researcher recommends that the governments use the proposed model to assess their information security preparedness levels periodically so that they can maintain highest level of information security readiness at any time. Completed assessment reports should provide a basis for an action plan undertaken by county governments to upgrade their information security practices. Each department concerned with information security in

e-governance should decide additional information security practices to be added to the system or customize the system to match their specific information security requirements.

It is also recommended that the government as a regulating agency impose compliance on periodic assessment of information security capabilities of their departments, counties and agencies. This process will motivate governments that are reluctant in reviewing and updating their information security practices to regularly update their security practices.

5.4.2 Recommendation for Further Research

The study dwelt mainly on information security situation in county government, therefore further research should be done in order to extend the applicability of this model in other organization. Further studies should also establish new approaches of assessing information security using specific international best practice for information security management in organizations such as ISO/IEC 27001, NIST cyber security framework among others.

REFERENCES

- Ahmad, W. Al, & Mohammad, B. (2012). Can a Single Security Framework Address Information Security Risks Adequately? *International Journal of Digital Information and Wireless Communications*, 2(3), 222–230.
- Alkalbani, A., Deng, H., & Kam, B. (2014). A Conceptual Framework for Information Security in Public Organizations for E-Government Development. *25th Australasian Conference on Information Systems*.
- Alshehri, M, & Drew, S. (2010). Implementation of e-Government: Advantages and Challenges. *Iask E-Alt2010 Conference Proceedings Vertical*, 79–86.
- Alshehri, Mohammed, & Drew, S. J. (2011). E-government principles : implementation , advantages and challenges Author advantages and challenges. *International Journal of Electronic Business*.
- Antwi, S. K., & Kasim, H. (2015). Qualitative and Quantitative Research Paradigms in Business Research: A Philosophical Reflection Performance Management Practices in the Ghanaian local government system View pro(N. Bindu, 2019)ject. *European Journal of Business and Management*, 7(3), 217–226.
- Awa, H. O., Ukoha, O., & Igwe, S. R. (2017). Revisiting technology-organization-environment (T-O-E) theory for enriched applicability. *Bottom Line*, 30(1), 2–22. <https://doi.org/10.1108/BL-12-2016-0044>
- Barrett, M. (2018). Framework for improving critical infrastructure cybersecurity. *Proceedings of the Annual ISA Analysis Division Symposium*, 535, 9–25.
- Bhattacharya, S. (2011). Study of E-Governance : The Attractive Way to Reach the Citizens. *International Journal of Computer Applications*, 29–33.
- Bhuvaneshwari, T., & Prabakaran, S. (2013). A Survey on Software Development Life Cycle Models. *International Journal of Computer Science and Mobile Computing*, 2(May), 262–267.
- Bisandu, D. B. (2016). Design Science Research Methodology in Computer Science and Information Systems. *International Journal of Information Technology*, November 2016, 1–6.
- Chadwick, A. E. (2017). Population/Sample. In M. Allen, *The SAGE Encyclopedia of Communication Research Methods*. SAGE Publications, Inc.
- Chen, S., Osman, N. M., Nunes, M. B., & Peng, G. C. (2011). Information Systems Evaluation Methodologies. *Proceedings of the IADIS International Workshop on Information Systems Research Trends, Approaches and Methodologies*, 22, 1–24. <https://doi.org/10.1186/1742-7622-5-2>
- CIPESA. (2015). *ICT in Governance in Kenya – Policies and Practice* (Issue 06).
- Creswell, J. W., & Creswell, J. D. (2017). *Research Design Qualitative, Quantitative, and Mixed Methods Approaches*. SAGE Publications, Inc.
- Edet, L. I., & Abasilim, U. D. (2015). E-Governance and Its Implementation Challenges in the Nigerian Public Serviv. *Acta Universitatis Danubius. Administratio*, 7(1), 30–42.

- Eduardo, A., & Junior, D. A. (2015). Adoption of Information Security Measures in Public Research Institutes. *Journal of Information Systems and Technology Management*, 12(2), 289–315. <https://doi.org/10.4301/S1807-17752015000200006>
- Federal Financial Institutions Examination Council. (2017). *FFIEC Cybersecurity Assessment Tool*.
- Government of Kenya. (2014). *ICT master plan*.
- Hassan, A. A. A. M. (2013). Information Security Management for Strategic and Effective Implementation of e-Management in the Governmental Institutions in Gaza. *Asian Journal of Business Information Management*, 20(13), 67–74.
- Heitkötter, H., & Majchrzak, T. A. (2013). Design Science at the Intersection of Physical and Virtual Design. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* (Vol. 7939, Issue April 2016). <https://doi.org/10.1007/978-3-642-38827-9>
- ICT Authority. (2016a). *Government Enterprise Architecture - Part 1 : General guiding principles*.
- ICT Authority. (2016b). *Information security standard- ICTA*.
- ISACA. (2012). *COBIT 5 ISACA's new framework for IT Governance, Risk, Security and Auditing*.
- Ismail, R., & Zainab, A. N. (2011). Information systems security in special and public libraries : an assessment of status. *Malaysian Journal of Library & Information Science*, 16(2), 45–62.
- ISO/IEC. (2005). *ISO/IEC 27001:2005 Information technology -- Security techniques -- Information security management systems – Requirements*. International Organization for Standardization and International Electrotechnical Commission.
- ISO/IEC. (2016). ISO/IEC 27000:2016(E) Information technology — Security techniques — Information security management systems — Overview and vocabulary. In *ISO.org [Online]: Vol. 4th Editio*. [http://standards.iso.org/ittf/PubliclyAvailableStandards/c066435_ISO_IEC_27000_2016\(E\).zip](http://standards.iso.org/ittf/PubliclyAvailableStandards/c066435_ISO_IEC_27000_2016(E).zip)
- ISO/IEC 27001. (2013). *ISO/IEC 27001: 2013 Information technology – Security techniques – Information security management systems – Requirements*. [file:///Users/anggraini/Documents/Mendeley Desktop/Normen-vereinigung - 2005 - Information technology – Security techniques – Information security management systems – Requirements.pdf](file:///Users/anggraini/Documents/Mendeley%20Desktop/Normen-vereinigung%20-2005%20-%20Information%20technology%20-%20Security%20techniques%20-%20Information%20security%20management%20systems%20-%20Requirements.pdf)
- Karokola, G. R. (2012). *A Framework for Securing e-Government Services The Case of Tanzania* (Issue 12). Stockholm University.
- Keung, Y. A. U. H. (2014). Information Security Controls. *Advanced Robot Automation, an Open Access Journal*, 3(2). <https://doi.org/10.4172/2168-9695.1000e118>
- Krishna, M. (2010). A Methodology for Measuring Information Security Maturity in Norwegian and Indian MSME 's with special focus on people factor. *Information Security*.
- Lee, K. A. (2008). *CS 2 SAT : The Control Systems Cyber Security Self-Assessment Tool*.

- Maryland Health Care Commission. (2019). *Cyber Security self-assessment tool*.
- Masau, F., Cheruiyot, W., & Mushi, C. (2011). *Trust and its challenges facing E-Government programs in Kenya*.
- Meiyanti, R., Utomo, B., Sensuse, D. I., & Wahyuni, R. (2019). E-Government Challenges in Developing Countries: A Literature Review. *2018 6th International Conference on Cyber and IT Service Management, CITSM 2018, April 2019*. <https://doi.org/10.1109/CITSM.2018.8674245>
- Miah, S. J., & Genemo, H. (2016). A Design Science Research Methodology for Expert Systems Development. *Australasian Journal of Information Systems*, 20, 1–29. <https://doi.org/10.3127/ajis.v20i0.1329>
- Ministry of ICT. (2018, February 05). *Ministry of Information, Communication and Technology*. Retrieved from Ministry of Information, Communication and Technology: <https://ict.go.ke/#>
- N. Bindu, C. P. (2019). From conventional governance to e-democracy: Tracing the evolution of e-governance research trends using network analysis tools. *Government Information Quarterly*, 385-399.
- Nadu, T. (2013). *E-Governance : A move towards paperless Administration in India*. 4, 404–411.
- National Institute of Standards and Technology. (2018). *Framework for Improving Critical Infrastructure Cyber security*. National Institute of Standards and Technology.
- National Institute of Standards and Technology. (2019). *NIST cyber security framework*.
- Nieles, M., & Dempsey, K. (2017). *An Introduction to Information Security An Introduction to Information Security*. NIST.
- NIST. (2019). *Baldrige cybersecurity excellence builder*. <https://www.nist.gov/system/files/documents/2019/03/24/baldrige-cybersecurity-excellence-builder-v1.1.pdf>
- Northcutt. (2019). *Security controls*. <https://www.sans.edu/cyber-research/security-laboratory/article/security-controls>
- Ochara, N. M. (2010). Assessing irreversibility of an E-Government project in Kenya: Implication for governance. *Government Information Quarterly*, 89-97.
- Otero, A. R. (2015). An information security control assessment methodology for organizations' financial information. *International Journal of Accounting Information Systems*, 18(266), 26–45. <https://doi.org/10.1016/j.accinf.2015.06.001>
- Ristov, S., Gusev, M., & Kostoska, M. (2011). Information Security Management System for Cloud Computing. *Encyclopedia of Cryptography and Security*, January, 607–607. https://doi.org/10.1007/978-1-4419-5906-5_1078
- Rouse, M. (2019). *Implementation*. <https://search.proquest.com/definition/implementation>
- Salam, M. A. (2013). *E-Governance for Good Governance through Public Service Delivery: An Assessment of District EService Centres in Bangladesh*. Dhaka, Bangladesh: Institute of Governance Studies, BRAC University.

- Scarfone, K., & Orebaugh, A. (2008). *Technical Guide to Information Security Testing and Assessment Recommendations of the National Institute of Standards and Technology*.
- Shareef, S. M. (2016). Enhancing Security of Information in E-Government. *Journal of Emerging Trends in Computing and Information Sciences*, 7(3), 139–146.
- Singh, A., Vaish, A., & Keserwani, P. K. (2014). Information Security: Components and Techniques. *International Journal of Advanced Research in Computer Science and Software Engineering*, 4(1), 2277–128.
- Singh, S., & Karaulia, D. S. (2014). E-Governance: Information Security Issues. *International Conference on Computer Science and Information Technology (ICCSIT'2011), December 2011*, 120–124.
- Smith, R. K. (2015). Chapter 2 -Some Well Known Software Development Life Cycle Models. In *Software Development Life Cycle Models* (pp. 1–15). <http://www.scribd.com/doc/21390992/Chapter-2-Software-Development-Life-Cycle-Models>
- Sommerville, I. (2010). *Software Engineering*. Addison Wesley.
- Stouffer, K., & Abrams, M. (2015). *Guide to Industrial Control Systems (ICS) Security NIST Special Publication 800-82 Guide to Industrial Control Systems (ICS) Security*.
- The Information commission office. (2019). *Data protection self-assessment*. <https://ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/>
- The Republic of Kenya. (2010). *The Constitution of Kenya, 2010*.
- UN Department of Economic and Social Affairs. (2016). *E-government Survey 2016*. United Nations. <http://unpan1.un.org/intradoc/groups/public/documents/UN-DPADM/UNPAN038853.pdf>
- Wamoto, F. O. (2015). E-government Implementation in Kenya , an evaluation of Factors hindering or promoting e-government successful implementation. *International Journal of Computer Applications Technology and Research*, 4(12), 906–915.
- Youker, B. B. W. (2010). *Goal-Free Evaluation and Goal-Based Evaluation*. <http://www.wmich.edu/evalctr/wp-content/uploads/2010/05/Youker-Fall-051.pdf>

APPENDICES

Appendix I: Questionnaire

Instructions

The questions below are for the purposes of assessing the security status of e-governance services offered by the counties. This will help the researcher in coming up with a model for determining organization information security preparedness levels. Your opinions as reflected in this questionnaire are important to this study and are held in confidentiality. Therefore, you are requested to fill this questionnaire in the freest and honest way possible.

SECTION A: General Background Information

Please kindly provide the following information. The information gathered will be kept strictly confidential and will only be used for the research and not for any other reason.

County Name:..... Date.....

Job Title:..... Department:.....

Your duties:

.....

.....

What is your highest academic qualification?

Diploma Degree Masters PhD Others (Please specify):

How long have you been working for this county?

Less than a year 1 – 2 years 2 – 5 years More than
5 years

Total working experience in the field of Information Technology:

Less than 6 years 6 – 10 years 11 – 15 years 16 – 20 years more than
20 years

SECTION B

The following is a list of Information Systems (IS) safeguarding measures. Please tick (√) in the box to indicate the level of implementation in your county government based on index below:

1 - Not implemented 2 - only some part has been implemented 3 - Implemented but has not been reviewed 4 - Implemented and reviewed on regular basis 5 - fully implemented and recognized as good for information security

Technological controls					
1. Access Controls	1	2	3	4	5
1. There is a documented access control policy that is communicated appropriately					
2. There are controls in place to ensure users only have access to the network resources they have been specially authorized to use and are required for their duties					
3. There is formal user access registration process and a formal user access provisioning process for assigning access rights for all user types and services					
4. There is a process to ensure user access rights are removed on termination of employment or contract, or adjusted upon change of role					
5. Access to information and application system functions are restricted in line with the access control policy					
2. System Software Security safeguarding measures					
1. There are established procedures which list all requirements with regard to outsourcing any county Information Systems service or activities.					
2. There are anti- spyware, anti-phishing and cleanup software solutions to detect, prevent and remove any spyware threats, phishing attacks and trashed files regularly.					
3. There is a rollback software to keep track and record any changes made to the computers and allow the system to be restored to its original state from any chosen point in time.					
4. There is a web filtering software to prevent access to inappropriate					

materials or sites.					
5. There is an application firewall is used for mobile laptops that connect to the county's LAN					
3. Network Security and Server Security safeguarding measures					
1. Firewall to protect the internal network from external threats and with virtual private network installed for remote and wireless access connections					
2. Use of wireless security products to secure the county wireless network. (Use of default passwords on wireless access points, network ID, wireless intrusion detection systems, wired equivalency protocol (WEP) encryption, MAC address filtering or virtual private networking (VPN))					
3. There is authentication systems to prevent unauthorized access to the county's server.					
4. There is routine backup for the data, safe storage of hard copy of server hardware specifications, installation information, installation software and passwords at an offsite location.					
5. The server is placed in a secure location, such as in a lockable cage, a locked room and place it with environmental controls.					
4. Data Security safeguarding measures					
1. There are data classification, retention and destruction procedures for handling county data, media or materials that contain county sensitive information.					
2. There are procedures on intellectual property rights and copyrights in controlling and protecting any digital works or resources that are stored, transmitted, accessed, copied or downloaded via the county information systems					
3. There are policies on sharing, storing and transmitting of county data via ISPs, external networks or contractors' systems.					
4. Use of cryptography techniques, hardware & software tokens and single sign on systems to control data access to the county internal and remote computer systems					
5. Vital County's business information or records are regularly backed up and stored in a different site.					

2. Organization Controls					
1. Human Resource Security safeguarding measures	1	2	3	4	5
1. Background verification checks carried out on all new candidates for employment and approved by appropriate management authority					
2. All employees and contractors sign confidentiality and nondisclosure agreements					
3. County executive members are engaged in driving security within the county and encourage, all employees and contractors to apply security in accordance with established policies and procedures					
4. There are formal disciplinary procedures which allows the organization to take action against employees who have committed an information security breach. Verbal warning, written warning, suspension or dismissal.					
5. There is a documented process for terminating or changing employment duties and is communicated to the employees and/or contractors					
2. Information Security Policy					
1. There are policies on access control authentication and authorization practices for using the county Information Systems.					
2. There are policies on protection of county assets to protect your county's hardware, software, data and people.					
3. There are polices on reporting, notification and response of Information Systems security events to affected parties such as citizens, law enforcement, and business partners.					
4. Policies on acceptable use of wireless devices in your county such as laptops and hand phones, workstations, e- mails, databases, intranet and Internet in your county.					
5. Procedures for update and review existing information security policies					
3. Awareness creation, training and education					
1. All staff at various levels are made aware of their responsibilities with regard to protecting the county's Information Systems' security and					

are also regularly trained to report any security breach incidences.					
2. All staff at various levels receive appropriate information security trainings and education on regular basis and routinely updated on county information security policies and procedures					
3. Information security awareness trainings is mandatory to all staff and patrons at various levels.					
4. There are balanced set of key performance indicators (KPIs) and metrics used to provide the real insight into the effectiveness of security awareness programs.					
5. There are positive supports and commitments from the top management to coordinate the implementation of Information Systems' security controls in your county. (Such as, allocation of budget, strong interest and active involvements).					

3. Environmental Controls					
1. Compliance					
1. The county has identified and documented all relevant legislative, regulatory or contractual requirements related to security					
2. All the records within the county are protected from loss, destruction, falsification and unauthorized access or release in accordance with legislative, regulatory, contractual and business requirements					
3. The county protects personal data in accordance with relevant legislation					
4. The county ensures that the implementation of security controls and information security is subject to regular independent reviews					
5. The county conducts technical compliance reviews of e-governance information systems regularly					
2. Physical and Environmental Security					
1. Lightning protectors and surge protectors to protect any valuable machines or equipment from lighting strikes, voltage spikes and surges.					
2. Security guards to monitor people entering and leaving the county buildings and sites					
3. Use of automatic sprinkler systems, smoke detectors, fire extinguishers					

and fireproof installations in the county buildings to detect and prevent fires, toxic chemical spills and explosions.					
4. Use of magnetic stripe swipe cards, electronic lock, proximity cards, bar code card or biometrics to secure and control access to restricted county areas.					
5. Air conditionings to stabilize the temperature & humidity within the county building.					

SECTION C: Information security preparedness indicators

The following is a list of Information security preparedness indicators. In your own view, please tick (√) in the box to indicate the overall level of implementation in your county government based on index below:

1 - Not implemented, 2 - partly implemented, 3 - Implemented but has not been reviewed, 4 - Implemented and reviewed on regular basis, 5 - fully implemented and recognized as good for information security

Information security preparedness indicators	1	2	3	4	5
1. Access controls					
2. Server and network security					
3. System software security					
4. Data security					
5. Human Resource Security					
6. Security awareness, training and education					
7. Information security policy					
8. Physical and environmental security					
9. Compliance					

Note: I would like to thank you for taking the time to complete this questionnaire. Your cooperation is highly appreciated.

Appendix II: Validity Tool

The following is a list of modules in the OISP model. In your own assessment, please tick (√) in the box to indicate the overall effectiveness of the module based on index below:

1 - Not effective, 2 - partly effective, 3 - effective

Module	Objective	Effectiveness			Remarks
		1	2	3	
User login and authentication	The model should prompt user to provide login credentials before being allowed to access the system components and only allow users who successfully provided username or email and password that matches those stored in the database.				
User session handling	The model should create sessions when users logs into the model, track all the user activities when the session is on, and destroys the session when the user logs out of the system.				
Information security assessment	The model should retrieve assessment questions from the database and present to the user in a Likert scale layout and also allow the user to submit duly filed assessment form to the database				
Reports module	The model should retrieve reports on assessment scores and recommendations and allow the user to view or download the results. Additionally, the administrator who is the CISO should be able to view all other users' assessment reports and the overall organization preparedness level.				
Settings	This module should only be accessible to the user with administrator privileges. It should				

	enable them to register other system users by assigning them roles according to their responsibilities in information security management and also add new roles. In addition, they should be able to add and modify the assessment questions depending on the adopted practices of the organization.				
OISP calculation	The model should compute the preparedness level as per submitted user scores and present the results to the user in percentage.				

Appendix III: Research Letter

Gladys Korir
Kabarak University
0719208720
gladyskorir94@gmail.com

The County Secretary
Uasin Gishu County Government
P.O Box 40-30100,
Eldoret.

Dear Sir/Madam,

Re: Permission to carry Out Academic Research

I am a Master of Science (Information Technology) student at Kabarak University-Nakuru conducting a research study entitled: **A Model for Determining Information Security Preparedness Level in E-Governance in Kenya's County Governments: Case of Uasin Gishu County Government.** The objectives of the research is to assess the existing security measures taken to secure e-governance services offered by county governments in Kenya and identify organization information security measures adopted by county governments to secure e-governance services thus coming up with an information security self-assessment tool for assessing the information security preparedness levels of county governments during e-governance implementation.

The purpose of this letter is to request you to kindly fill in the questionnaire with precision and accuracy. The questionnaire is supposed to assist in answering specific objectives of the research which is being undertaken as part of the University requirement. Any information given herein will be treated with utmost confidentiality and only be used for the purpose of research. So kindly feel free to fill the questionnaire.

Thank you

Yours Faithfully,

Gladys Korir

Appendix IV: University Research Permit



INSTITUTE OF POST GRADUATE STUDIES

Private Bag - 20157
KABARAK, KENYA
E-mail: directorpostgraduate@kabarak.ac.ke

Tel: 0203511275
Fax: 254-51-343012
www.kabarak.ac.ke

30th Aug 2017

Ministry of Higher Education Science and Technology,
National Council for Science, Technology & Innovation,
P.O. Box 30623 - 00100,

Dear Sir/Madam,

RE: RESEARCH BY GLADYS KORIR – GDI/ON/0143/01/16

The above named is a student at Kabarak University taking Masters Degree in Information Technology (IT). She is carrying out research entitled "*A framework for information security for E-governance implementation in Kenya county Governments: A case of Uasingishu county government.*"

The information obtained in the course of this research will be used for academic purposes only and will be treated with utmost confidentiality.

Please provide the necessary assistance.

Thank you.

Yours faithfully,

Dr. Betty J. Tikoko
DIRECTOR - (POST-GRADUATE STUDIES)



Kabarak University Moral Code

As members of Kabarak University family, we purpose at all times and in all places, to set apart in one's heart, Jesus as Lord. (1 Peter 3:15)

Appendix V: Introduction Letter

REPUBLIC OF KENYA
COUNTY GOVERNMENT OF UASIN GISHU
DEPARTMENT OF EDUCATION, CULTURE, YOUTH AFFAIRS, SOCIAL SERVICES & SPORTS
OFFICE OF CHIEF OFFICER EDUCATION, CULTURE AND SOCIAL SERVICES

Email: @uasingishu.go.ke

Tel. NOs: 053 2033737
+254-053-2061330
+254-053-2032603
+254-053-2062208

Fax: +254-053-2062884
Website: www.uasingishu.go.ke



When Replying, Please Address to:
Chief Officer, Education, Culture and Soci
Services
County Government of
Uasin Gishu
P. O Box 40-30100
ELDORET-KENYA

17TH JULY, 2018

GLADYS KORIR
KABARAK UNIVERSITY



RE: PERMISSION TO CARRY OUT ACADEMIC RESEARCH

Following your letter of request to carry out research within the County on “A framework for information security for E-Governance implementation in Kenya’s county governments”.

You are hereby given authority to do so.


ROSELYN KOSGEI
AG. CO. EDUCATION, CULTURE AND SOCIAL SERVICES

Copy: COUNTY SECRETARY
HEAD OF PUBLIC SERVICE

Appendix VI: NACOSTI Authorization Letter



NATIONAL COMMISSION FOR SCIENCE, TECHNOLOGY AND INNOVATION

Telephone: 020 400 7000,
0713 788787,0735404245
Fax: +254-20-318245,318249
Email: dg@nacosti.go.ke
Website: www.nacosti.go.ke
When replying please quote

NACOSTI, Upper Kabete
Offi Waiyaki Way
P.O. Box 30623-00100
NAIROBI-KENYA

Ref. No. **NACOSTI/P/17/05408/19941**

Date: **15th November, 2017**

Gladys Jebet Korir
Kabarak University
Private Bag - 20157
KABARAK.

RE: RESEARCH AUTHORIZATION

Following your application for authority to carry out research on "*A framework for information security for e-governance implementation in Kenyan County Governments: A case of Uasin Gishu County*" I am pleased to inform you that you have been authorized to undertake research in **selected Counties** for the period ending **14th November, 2018**.

You are advised to report to **the County Commissioners, the County Directors of Education and the County Executives, selected Counties** before embarking on the research project.

Kindly note that, as an applicant who has been licensed under the Science, Technology and Innovation Act, 2013 to conduct research in Kenya, you shall deposit a **copy** of the final research report to the Commission within **one year** of completion. The soft copy of the same should be submitted through the Online Research Information System.

**GODFREY P. KALERWA MSc., MBA, MKIM
FOR: DIRECTOR-GENERAL/CEO**

Copy to:

The County Commissioners
Selected Counties.

The County Directors of Education
Selected Counties.

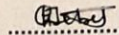
Appendix VII: NACOSTI Research Permit


THIS IS TO CERTIFY THAT:
MS. GLADYS JEBET KORIR
of **KABARAK UNIVERSITY, 0-30100**
Eldoret, has been permitted to conduct
research in Nakuru , Uasin-Gishu
Counties


Permit No : NACOSTI/P/17/05408/19941
Date Of Issue : 15th November, 2017
Fee Recieved :Ksh 1000

on the topic: A FRAMEWORK FOR
INFORMATION SECURITY FOR
E-GOVERNANCE IMPLEMENTATION IN
KENYAN COUNTY GOVERNMENTS: A
CASE OF UASIN GISHU COUNTY

for the period ending:
14th November, 2018



.....
Applicant's
Signature





.....
Director General
National Commission for Science,
Technology & Innovation

CONDITIONS

1. The License is valid for the proposed research, research site specified period.
2. Both the Licence and any rights thereunder are non-transferable.
3. Upon request of the Commission, the Licensee shall submit a progress report.
4. The Licensee shall report to the County Director of Education and County Governor in the area of research before commencement of the research.
5. Excavation, filming and collection of specimens are subject to further permissions from relevant Government agencies.
6. This Licence does not give authority to transfer research materials.
7. The Licensee shall submit two (2) hard copies and upload a soft copy of their final report.
8. The Commission reserves the right to modify the conditions of this Licence including its cancellation without prior notice.


REPUBLIC OF KENYA


National Commission for Science,
Technology and Innovation
RESEARCH CLEARANCE
PERMIT

Serial No.A 16504
CONDITIONS: see back page

A Model for Assessing Information Security Preparedness Level in E-Governance in Kenya's County Governments

Gladys Korir
Kabarak University

Abstract:- The purpose of the study is to discuss fundamental information security control measures that can be used to develop a model to determine organization information security preparedness level. The model utilizes a web-based platform containing specific information security indicators against which governments can assess their capability to protect e-governance systems. The study adopted design science research methodology to implement the model. The target population were selected based on their knowledge, experience and roles in e-governance. The study adopted cluster and simple random sampling methods. To evaluate the model, a goal-based approach was used. The study established that technological, environmental and organization controls measures directly contribute to organization information security and that their individual implementations level affects the security posture of an organization. The study provides a method by which governments can use to assess their information security control measures and hence work towards improving their organizational information security posture.

Keywords:- E-Governance, Information Security, Information Security Control Measures, Organization Information Security Preparedness.

I. INTRODUCTION

In an age where globalization and emerging technologies have taken root of every aspect of life, governments are now obligated to use new emerging and disruptive technologies to deliver public services. Governments are continually relying on information systems for efficient, accountable and transparent public service delivery (Nadu, 2013). E-governance is becoming a formal way of providing improved public services. The resultant benefits of e-governance are less corruption, increased transparency, greater convenience, revenue growth, and cost reductions (Wamoto, 2015). Countries globally are increasingly taking up on utilization of ICTs to deliver public services, increase transparency and engage people in decision-making processes. According to the United Nations E-Government Survey 2016, there has been an inclined rise in the number of countries utilizing advanced electronic and mobile services to provide public services online through one-stop platforms.

In Kenya, electronic governance has been supported momentarily as an ideal remedy for improving governance and enabling other critical functions of the government (Ochara, 2008). In 2004, the Kenyan government approved the e-government plan marking the start of e-governance journey in Kenya (Wamoto, 2015). Since then, the government of Kenya has initiated several e-governance systems with the aim of enhancing efficiency, transparency and democracy within public administration. The implementation of these systems however, has encountered several challenges, which include technical challenges –like security and privacy of information, inadequate infrastructure, financial challenges due to inadequate funding, social issues and human challenges (Meiyanti et al., 2019).

Security and privacy of information is a major technical challenge facing e-governance initiatives in Kenya (Wamoto, 2015). Citizens' concerns about their information and transactions privacy is one of the major factors influencing the success of e-government initiatives. Information security is a critical element in the implementation of any e-governance initiative (Shareef, 2016). Information security ensures that the confidentiality, integrity and availability of information are protected. In Kenya, information security in e-governance have been addressed using different approaches but still appear to be weak. For instance, the government of Kenya was reported to have lost over \$171million to cyber-crimes by the end of 2017, which is said to be the highest record in East Africa (Cisco, 2017). Today's governments and organizations employ very sophisticated security tools and technologies like firewalls, encryption, access control management, and others to curb this challenge. While advanced security technologies are fundamental parts of operational information security practices, it has been observed that appropriate security technologies alone are not adequate in addressing information security challenges (Otero, 2014).

In order to enhance information security, governments and organizations need to evaluate their information security practices on a regular basis so as to determine their security capability and thus review and update their information security practices to satisfy their specific security requirements and to overcome the challenge of the dynamic nature of information security threats (Otero, 2014). Enhancing information security in e-governance not only nurture secure e-governance services, but also, builds confidence and trust in e-governance system users (Masau et al., 2011); leading to the success of e-governance initiatives (Karakola, 2012).

Appendix IX: Evidence of Conference Participation

