# AN IMPLEMENTATION FRAMEWORK FOR EFFECTIVE INFORMATION SECURITY CONTROL SYSTEMS IN TVETI IN NAIROBI COUNTY KENYA

**BY**

**RACHAEL WANGUI KIROKO**

**BED. (Kenya Methodist University)**

**A RESEARCH THESIS SUBMITTED TO THE SCHOOL OF POST-GRADUATE STUDIES IN PARTIAL FULFILLMENT FOR THE AWARD OF THE DEGREE OF MASTER OF INFORMATION SYSTEMS OF THE SCHOOL OF INFORMATION SCIENCE AND TECHNOLOGY, DEPARTMENT OF COMPUTING SCIENCES**

**KISII UNIVERSITY**

**SEPTEMBER, 2020**

# DECLARATION

This thesis is my original work and has not been presented for a degree award in this or any other university.

Racheal Wangui Kiroko

MIN11/20342/14

Signature: ……………………… Date: ……………………

This thesis has been submitted for consideration with our approval as University

Supervisors:

Dr James Ogalo,

Faculty of Information Sciences and Technology, Kisii University

Signature: ……………………… Date: ……………………

Associate Prof.Felix Musau

Faculty of Information Sciences and Technology, Riara University

Signature: ……………………… Date: ……………………

# PLAGIARISM DECLARATION

I declare I have read and understood Kisii university rules and regulations, and other documents concerning academic dishonesty. I do understand that ignorance of these rules and regulations is not an excuse for a violation of the said rules. If I have any questions or doubts, I realize that it is my responsibility to keep seeking an answer until I understand. I understand I must do my own work. I also understand that if I commit any act of academic dishonesty like plagiarism, my thesis can be assigned a fail grade. I further understand I may be suspended or expelled from the University for academic dishonesty.

Racheal Wangui Kiroko

MIN11/20342/14

Signature: ……………………… Date: ……………………

We declare that this thesis has been submitted to plagiarism detection service. The thesis contains less than 20% of plagiarized work. We hereby give consent for marking.

Dr.James Ogalo,

Faculty of Information Sciences and Technology, Kisii University

Signature: ……………………… Date: ……………

Associate Prof.Felix Musau

Faculty of Information Sciences and Technology, Riara University

Signature: ……………………… Date: ……………………

# WORD DECLARATION

I confirm that the word length of the thesis is….23,835..........,the thesis including footnotes is…23060……….and the appendices are…775…………I also declare the electronic the electronic version is identical to the final, hard bound copy of the thesis and corresponds with those on which the examiners based their recommendation for the award of the degree.

Racheal Wangui Kiroko

MIN11/20342/14

Signature: ……………………… Date: ……………………

We confirm that the thesis submitted by the above named candidate complies with the relevant word length specified in the School of Postgraduate and Commission of University Education regulations for the master's degree.

Dr James Ogalo,

Faculty of Information Sciences and Technology, Kisii University

Signature………. Email……………. Tel: …………. Date: ………….

Associate Prof. Felix Musau

Faculty of Information Sciences and Technology, Riara University

Signature……… Email……………… Tel............. Date……………

# COPY RIGHT

# DEDICATION

Am dedicating my thesis to two people I value most, firstly my husband and secondly my son who have played a big role in my whole period of my study, encouraging me, morally financially, they are my greatest pillar of my life.

# ACKNOWLEDGEMENTS

All my gratitude goes to the Almighty God for keeping me alive this far and for enabling me to carry out this research. The successful completion of this research has been possible because of the effort of several people. My sincere regards goes to Dr. Ogalo and prof.Musau, who supervised me with a lot of motivation, concern, encouragement and for the continuous support of my research. Their guidance and direction in research of this thesis is highly appreciated. I also thank the friends, my family for word of encouragement especially my dear husband and my son for supporting me spiritually and economically throughout my life. I also appreciate the contribution of the respondents for the co-operation in filling out the questionnaires. While acknowledging the help of all the above, I take responsibility for any errors that still remain in this thesis. God bless you all.

# ABSTRACT

Information security control system involves all the activities which are used in directing and controlling all the security control operations maintaining security of data in the technical institutions. The effective data control system in education has the potential to enhance the quality of information and data, the research productivity of staff, students and effectiveness of institutions. Private and public colleges have adopted measures in the area of information security; this has been done through use of recommended standards and guidelines that have been put in place to ensure that security is enhanced for effective Information Security Control Systems. The difficulties facing Technical, Vocational and Education Training Institutes mainly is how they can protect and manage their information control systems effectively that support teaching, learning and research activities. This thesis sought to develop an implementation framework for effective information security control systems in private and public Technical, Vocational and Education Training institutes (TVETI) in Nairobi County. The study sought to determine the effects of security policies, impact of security awareness, information security access methods and information security environment practices as the objectives of the research for effective information security control systems in private and public colleges in Nairobi County. The study targeted a population of 714 security Experts of information security in private and public colleges in Nairobi County with a sample size of 216 ICT security Experts respondents. Questionnaires were used for collecting data; both qualitative and quantitative research designs were used. Data collection and analysis depend upon; the study suggested a framework that is required to give a full implementation model for increasing the level of agreement amongst end-users, with the purpose of checking, measuring and evaluating to users' behavior with data security policy. The proposed method depends upon on two crucial ideas: taxonomy of the response plan to non-agreeable behavior, and a agreeable points system. The response taxonomy is consisted of two groups:  awareness increment and data security policy enforcement. The agreeable points system is used to reward agreeable behavior, and punish non-agreeable behavior. This study concluded that there are many security threats and gaps in these institutions information security control practices adopted in private and public colleges in Nairobi County. The study recommended that the private and public colleges need to come up with security policies and adapt the proposed implementation framework to boast the safety and effectiveness of their information security control systems. Understanding the factors influencing effective information security control systems in teaching in private and public colleges was important as it would provide the entire education institutions with information regarding the adaption of effective information security control systems in public and private colleges in Nairobi County. This research is to help information security practitioners to come up with new security practices so as to have security of their systems by adapting the recommended security measures and security access controls methods. This would help to improve information security control systems by eliminating several security breaches and gaps in information security management in private and public colleges in Nairobi County.

# TABLE OF CONTENTS

CHAPTER THREE

CHAPTER FOUR

CHAPTER FIVE

## LIST OF TABLES

# LIST OF FIGURES

# ABBREVIATIONS AND ACRONYMS

**DMZ**-Demilitarized Zone

**ICT-**Information Communication Technology

**ISA**-Information System Audit

**ISAC-**Information Security Access Control

**ISC**-Information Security Control

**ISCM**-Information Security Continuous Monitoring

**ISCS-**Information Security Control System

**IT-**Information Technology

**TVETI**-Technical, Vocation and Education Training Institutes

**VPN-**Virtual Private Network

# CHAPTER ONE

## 1.0 INTRODUCTION

### 1.1 Background to the study

All the activities which are meant to ensure that security of data is provided effectively in all private and public colleges are known as data protection and control as cited by (nieles, et-al, 2017).

Private and public colleges do their daily routine activities using information technology (IT), hence exposed them to so many security threats and risks. Various private and public technical colleges make use of technology to enable distant learning (e-learning) in removing geographical and reducing cost of higher education which pose technological assets at security risk in Kenya education institutions (Ministry of Higher Education, 2007).

Private and public colleges have adopted methods for data protection; which has been done through usage of recommended standards and guidelines necessary for the establishment, operation and maintaining effective Information Security Control Systems. The recommended standards include ISO 9001:2015, ISO 9001:2008 and ISO/IEC 27001 (Arnason and Willet, 2008).

In Canada, in their Internal Audit Final Report (2017) stated that purpose of an audit is to make the information security control systems well protected and properly secured by the use of the best frameworks to prevent unauthorized and unauthenticated access according to the set standards, guidelines and procedures in different education institutions.

The control systems that secure information in most of private and public colleges have been missing, and where these systems have been put in place and used, their effectiveness in securing information control systems in private and public colleges has not been very good.

There is high chance that majority of education institutions are exposed to many possible threats whose source may be occurring internally or externally to the organization. (Calder and Watkins, 2008),

(Chaulaa, et-al, 2017) stated that auditing and checking of institutions security threats is a way of establishing, collecting, analyzing various operations and prevention from all threats, which provide high level of trust that shows how good the system is to meet the required security level and acceptable by all the users of the security control systems, considered as data protection confidentiality in private and public colleges in Nairobi County. Further suggested the security assurance is expensive and require a lot of time in establishing security policies, guidelines, methods and procedures, considered to be important in private and public colleges in Nairobi County. The technical education and vocational institutions all their operational activities and procedures are required to be secured to enhance confidentiality and integrity of the information in those technical college institutions. RMAS,( 2017) the Information Security Audit helps private and public colleges in Kenya to mitigate security risks and during audit process it covers education institutions usage, functionality,practices,procedures and all related data protection issues. During the evaluation, checking and monitoring on the information security control, the involved Security Audit team on all practices, policies and procedures on how they affect all information security control activities and whether they impact positively or negatively to those education institutions. Monitoring and auditing is of the importance to meet the aim of effective information security control within these technical institutions.

This is achieved through use of recommended framework, internationally accepted guidelines and procedures for effective information security control.

(Steinbart et al. (2013) when he collected some data in different organizations stated that all the expert people concerned with data security were in agreement that ensuring that the recommended framework, checking frequently the policies, practices and procedures was very necessary in private and public colleges to ensure highly enhanced threats prevention and control.

The importance of doing this practice go hand in hand in improving both the workers and all using the security systems acceptance and maintenance in one particular institution, also these data experts emphasized the practice of giving out the result findings pertaining the level of security enhancement was very crucial in maintaining good data security and helping effective security control systems in private and public colleges in Nairobi County.

(Steinbart et al, 2013) when he made some investigations of the data protection experts in various organization stated that improved corporation of data protection guidelines with the usage of the recommended practices, procedures and also better altitude of these data prevention experts boast effective data control systems in private and public colleges in Nairobi County.

Successful information security control systems should have a lot of good security infrastructures and workers user protection awareness pertaining data risky issues faced in public and private colleges in Kenya.

(CIO East Africa, 2012) stated that an Indonesian university IT expert cracked several government security systems within one night, employees have contributed greatly towards data breach faced by institutions.

Information security systems have continued to change continuously, making information security control systems more difficult and challenging to secure in private and public colleges in Kenya.

According to Arnason and Willet (2008), there are many incidents that demonstrate the information security control systems currently in use are ineffective or lack of information security policies in some of the Kenyan institutions. He further stated that, best practices in information security control recommend that information security control guidelines, procedures and policies are established to have effective security control systems in private and public colleges in Kenya.

User's permission to access the security control systems should be determined by individual recognition, permitted and right people required to use these systems by making using of several authenticating methods like passwords which are secretly known by an individual, or use of a smartcard or the use of fingerprint identification.

(Musa,2014,Stolarski, 2012) argued that threats protection can be enhanced by use of strong barriers, like strong entry points, good identification mechanisms to deter malicious people and hackers of security control systems in private and public colleges in Kenya. Further stated that to establish best recommended authorization, authentication mechanisms and strong information access control methods, there is need for all the people in management level to strongly provide the necessary support and proper enforcement of secure information security control systems in private and public colleges in Kenya.

He further said most of the institutions should have total control data protection; some of these data protection methods involve use of secretive individual password, a well-protected smartcard and use of biometric sensors to enhance and improve information security control systems.

Understanding security control systems operations is useful for this technical knowhow may facilitate  adaption of effective information security control systems and encourage effective information security control systems in public and private colleges in Kenya education institutions. This study therefore sought to develop an implementation framework for effective information security control systems in public and private technical colleges in Nairobi County.

## 1.2 Problem Statement

One of the greatest problem facing Technical, Vocational and Education Training Institutes is difficulties and challenges they face in protecting data by reducing complex threats and risks evolving continuously to have effective information and data protection established in all their operations and functionality control systems on daily bases in these technical college institutes. They lack structured implementation framework for managing effectively information security control systems in these institutions (Deloitte East Africa, 2011).

Another challenge facing these institutions of higher learning is of malicious workers who use the technological assets to do work that benefit themselves and not the institution (CIO East Africa, 2014).

Kenyan institutions of higher learning are very vulnerable and have faced one of the highest attacks, leading the institutions in suffering greatly due to these attacks in Africa.  Institute's recommended data protection against risks and threats facing them need to be efficient.

The established protective data and control would help to provide necessary security expected in those systems at any one time in these institutions, many tutors, lecturers and trainers have suffered from their information security breach committed by some of the students they teach and have acquired more skills in computer science than them, some accessing their academic grades altering, them and lack of secure Web transactions in their systems.

The security control systems have no secure socket layer (SSL) that is put in place, lack of procedure for Access Rights Review put in place, lack of monitoring for unauthorized activities to the sensitive information, lack of protection of information systems and Employee orientation for information and IT security were major issues affecting effective information security control in Technical Training Institutes in Nairobi County, information security service provider Cyberoam (2015).

### 1.3 The Purpose of the Study

This research study proposed to develop an implementation framework for effective information security control systems in Technical, Vocational and Education Training Institutes in Nairobi County.

### 1.4 Objectives of the Study

1. To determine how the college security policies affect Information security control systems in Technical, Vocational and Education Training Institutes in Nairobi County.

2. To establish the impact of security awareness on Information security control systems in Nairobi Technical Training Institutes.

3. To examine how the information security access methods influence Information security control systems in Technical Training Institutes in Nairobi County.

4. To establish how Information system environment practices affect Information security control systems in Technical Training Institutes in Nairobi County.

### 1.5 Research Questions of the Study

This research study was designed to answer the research questions listed below.

1. How are college security policies affecting Information security control systems in Technical Training Institutes in Nairobi County?

2. What are impacts of security awareness affecting Information security control systems in Nairobi Technical Training Institutes?

3. How are information security access methods influencing Information security control systems in Technical Training Institutes in Nairobi County?

4. How are Information system environment practices affecting Information security control systems in Technical Training Institutes in Nairobi County?

### 1.6 Significance of the Study

The difficulties and hindrances encountered in College of maintaining effective information security control systems are the main reason of this study.

In the Institutes of higher learning, most studies of managing information security have been done in the universities, while technical training institutes has received little academic research focus.

This research is to enable information security professionals in technical training institutes to come up with new security practices and policies so as to ensure security control effectiveness of their information security infrastructures by adapting the recommended best practices and the proposed implementation framework.

This would help to improve information security control systems by enhancing their security always in private and public education technical institutes in Nairobi County.

## 1.7 Assumptions of the Study

This research study was done through the assumption that technical training institutes in Nairobi County have adopted information security control systems and the respondents were to provide accurate, truthful and honest responses in the questionnaires to be provided.

## 1.8 Scope of the Study

This research study was restricted to Technical Training Institutes in Nairobi County which have a mixture of different setting this includes: pre-university, technical and Satellite Campus settings.

## 1.9Limitations of the Study

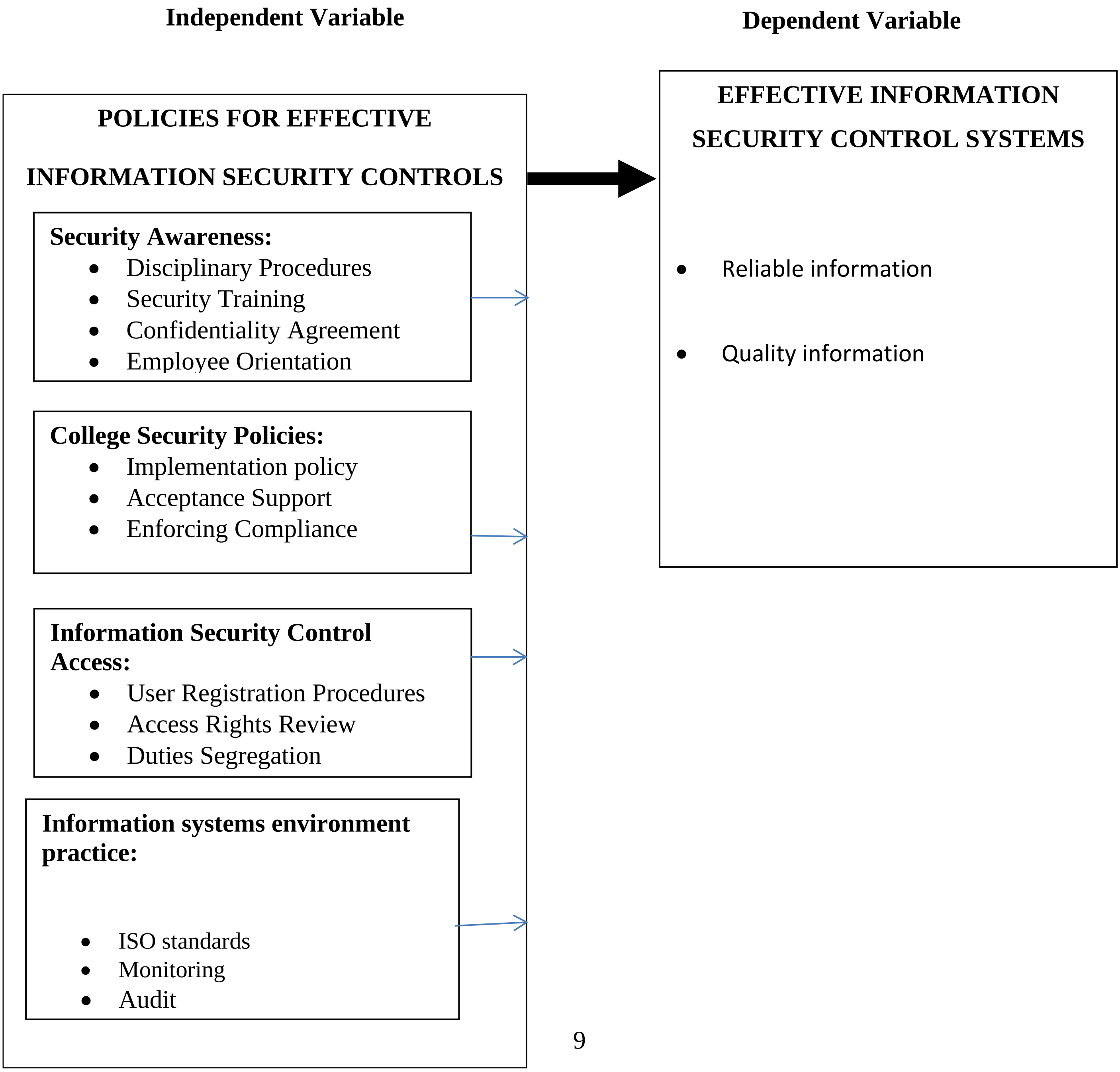
Limitations refer to the constraints or drawbacks both theoretical and practical that the researcher may find and has little or no control over (Orodho, 2004). The researcher acknowledges specific limitations of this study which include the reliance on individual respondents' willingness to complete the questionnaires provided with honesty in their responses.

This research study respondent's cooperation enhanced the provision of the required responses without biasness.  The study did not suffer any bias conditions, the researcher assured the respondents of individual responses confidentiality, also that their responses were meant to be used in this research study only.

### 1.10 Conceptual Framework

The conceptual framework shows the various factors that were influencing effective information security control systems in public and private colleges in Nairobi County. These variables included security awareness, security control access methods, security policies, and information security systems environment practices.

**Conceptual Framework of the Study**



## 1.11 Operational Definition of Terms

**Asset:** A resource used in Nairobi Technical training institutions such as computer system or the data it holds, used in learning and transmitting information within and outside in all these institutes in daily bases.

**Authentication**: The information security control access method used in technical training colleges in Nairobi County for checking that users are who they claim to be when accessing onto security information control systems.

**Authorization:** Determining whether user should have access to resources in the security information control systems in technical training institutes in Nairobi County. An effective information security control access method of permitting only authorized user accessing to important information by using the appropriate security authority have been put in place in these.

**Phishing**: High-tech scam that hackers of information security control systems in Nairobi institutes are deceiving employees into giving freely personal and private important data in these institutions using their emails or websites .

**Threats:** The confidentiality, integrity, availability, or authorized use in the technical institutions in Nairobi County has been be highly compromised by actions or events that have occurred in their information security control systems.

# CHAPTER TWO

# 2.0 LITEREATURE REVIEW

## 2.1 Introduction

This is concerned with previous findings of other literature done locally, nationally and internationally of security control systems and information security management systems in public and private colleges in Nairobi County. These included theories that shed security control principal facts, the benefits and aim of the study, objectives, recommendations, challenges and main findings which were found out from the beginning of security control systems establishment in academic and administrative activities in technical training institutes. Information (Riley, 2012) Stated that Communications and Technology (ICT)systems is involved with all activities related with electrical digital information and data platform ,including information systems and digital computers which require information security control systems.

## 2.2Theoretical Framework

The effective information control system in education is able to uplift the quality of data and information, the research productivity of staff, students and effectiveness of institutions (Kashorda, 2007). This implies that the study on information security systems and adaption in colleges cannot be exhausted without considering administrative support, environmental factors and the availability of resources.

As a guide to this study the Open Systems Model, Control and auditing theory, Technology Acceptance Model theory, Information Technology System Implementation process theory, were used.

### 2.2.1 Open Systems Theory

The institution is composed of both structures and fuctions,also constituted of categories of people, who forms individual who should help one another to perform duties together every individual should be aware the performance of the other. (Owens & Steinhoff, 1976) stated that every individual should be able to receive information, which they should be ready to adhere too. In the open systems theory, the college being a typical example of an organization is composed of Sub-systems: personal, technology, role and structural

In the institutions the mini-system is composed of lecturers, and IT security staffs, who deliver instructions, develop security systems and review security control systems continuity. Various orderly security procedures are important when carrying out several activities effectively without affecting information protection.

The institution should have information working assets to perform their roles and functions. The schools Subsystem interact with the external environment in such a manner that bringing change in one would necessarily lead to changes in all the others.

Therefore when considering the introduction of innovations in colleges, it is prudent to take cognizance of the inter-dependencies and interactive first between the four Subsystems and secondly with the external environment institutes: (i) check, help, and protect institutional transmission (i.e., information transmitted or received by institutions systems) at the external partitions and key internal partitions of the systems; and (ii) employ architectural designs, software development techniques, and systems engineering principles that To promote effective data security control within the institution architecture require checking ,auditing and securing internally and externally of the systems by implementing recommended standards and good implementation framework.

An information infrastructures principle provides the direction on various ways of protecting information security controls systems to achieve higher levels defence of information security in different subsystems. The Subsystems are thus important structures when trying to bring different approach in an institution. This theory was thus used to study effective information security control systems in public and private colleges in Nairobi County.

### 2.2.2 Control and Auditing Theory

Control and auditing theory is in the opinion that institutions need to have data protection and control systems. The control performance measures require to be done through various methods which include monitoring, auditing and evaluation. Several researchers who have conducted a survey in the area of data protection confirmed that effective data protection and management result to smooth data processes and protection against data threats and risks. For example, Weber (1999) stated that data protection and control measures help to prevent, check and prohibit cracking and hacking of the data protective systems in the institutions.

ISO/IEC 17799 investigation for data protection and control measures involves the data protection practices, procedures, guidelines and standards recommended internationally to reduce the threats and security risks of data within the institutions. Various recommended international standards in use to protect data from intrusion by hackers when effectively implemented and managed to facilitate the secured flow of data within the institution. The standards and guidelines for data protection, processes, procedures, infrastructures and workers help to achieves institutions functions effectively through reducing the risk, and coordinating and prevention measures. (COBIT, 1998) stated that should make use of data protection standards  effectively and have data protection strategies to be used always in all institutions activities and functions, regular monitoring, evaluation and auditing is necessary.

### 2.2.3 Technology Acceptance Model

To guide the study the Technology Acceptance Model theory was also used to predict and explain effective usage of data protection and control systems of the authorized people altitude to embrace or failure to accept the usage of data protection and control measures. The theory gives the user’s perceptions about the usage of the systems that is, the way the user embraces the system (Davis, 1989). It is concerned at the opinion of the users which forecast at what each person altitude of interacting with a particular system would improve the processes and the opinion of the workers in the institutions. The higher the degree of acceptance of the data protective practices, the higher the data protection and control measures.

### 2.2.4 I.T. System Implementation Model

This Model is concerned with the institution desire to achieve through new adaption of recommended data protective devices. This model aimed to provide proper coordination, processes and implementing framework for effective security control systems. There are six stages in this framework which ensure effective implementation .The aim of this phase help to discover the difficulties associated with the data protection and control, also an opportunity for improvement is done. Organizational adoption stages are achieved because of the management, workers practices and procedures to be used by the institutions. the motivation patterns ,the size, goals, understanding of an institution climate would facilitate the usage and creating a conductive environment for adoption of data protection and risk control.The initial level is where the users begin to learn and accept the new methods of data protection procedures, guidelines and practices gaining a better understanding and insights of how data protection and their daily activities need to be propely coordination to achieve the expected results in the organisation.

The reason of initial level is to prepare the institution to adopt the procedures of data protection successfully. This is actually achieved by discussion method that aim to make sound decisions for required assets to be provided neccssary for data protection activities.Routinization reflects the adjustment of organizational governance systems to improve the IT such that the it is not seen as new or  extra ordinary thing. Infusion is defined as the procedure of incoperating an IT application fully within an individual's or organization's work security control systems.Full and effective use of data protection and control measures in daily practice is acquired by prioritizing the objectives and processes of the institutions. It also facilitates effective data protection always.(Cooper and Zmud, 1990).Open Systems Theory, control auditing theory and Technology Acceptance Model (TAM) has not included the other external factors that may affect the implementation of data protection control systems (Jeyaraj et al., 2006).

Studying non-adopters of security control systems and factors influencing effective security control systems give a better perspective and ideas pertaining the other external factors that may affect good practices of data protection, such as the altitude, the pre-beliefs and prejudices of appropriate data protection and control through use of IT System Implementation Model.

## 2.3Empirical Literature Review

Various studies reveal a number of policies influencing information security control systems in public and private colleges in Nairobi County. The success for the information security control systems is determined through a dynamic process involving a set of interrelated factors. The importance of data protection and control is to maintain security systems and technological assets in technical training institutes in Nairobi County (Ismail et al., 2011).

However, it is very important for security professional trainers and policy makers to understand the factors for effective and cost-effectiveness of different approaches to security systems used in security professional training, also training strategies which can be appropriately explored to make such changes viable to all private and public colleges (Voogt and Knezek, 2012).

### 2.3.1 Security Policy

Information security policy is an important aseptic in developing positive information security practices in an organization. Box &Pottas (2013) stated that workers' know how and altitude of information security control practices influences the protection and control behavior, eventually the threat protecting patterns.

They further emphasized that employee's awareness on security information control practices results to better perspective by the employees, hence reducing security systems risky behavior (Parsons et al., 2014).

The statement is supported by Bulgurcu et al., (2010) who asserted that if there is positive perspective of information security by employees; it would facilitate and help to have a condition in which security control systems are well protected and secured from all threatening practices, Peltier et al. (2005), mentioned that foundation of well secured systems is having good documented procedures and practices.

Procedures and regulations utilized by all users of security control systems that interact with them should adhere to in the institutions.(Peltier et al., 2005). Further, Calder & Watkins (2008) highlighted that the best recommended practices and laid down procedures should be written, provided and accepted by workers at all levels and also the approval by management.

### 2.3.2 Security Awareness

Arnason& Willet (2008), stated that the protection and maintenance of technological assets is determined by the workers know how and awareness training pertaining all technological assets. It’s the management responsibility to state appropriately the security purpose and the workers specific functions should be well stated concerning the requirements of employment. Moreover, Calder & Watkins (2008) highlighted that an organization should carry out employee orientation awareness about information and information technology security.

Also developing and enhancing disciplinary rules and regulations for workers committing threatening security actions. Further, Arnason and Willet (2008), argued that appropriate standards need to be provided at the recruitment stage, when giving contracts and when employing specific people.

Before employment, organizations must make sure that all employees and other outside users comprehend their roles, and are competent for those responsibilities they are entitled, hence reducing the risky behavior or misuse of facilities. Newly employed should be properly scrutinized, especially for most important jobs.

When recruiting, Organizations must make sure that all inside workers and other outside users are well informed of information security risks, their roles and actions, and should protect organizational security policy at all times when working, and ensure that threatening issues are reduced (Arnason and Willet, 2008).

Corporate Technology Group (2008), The most destructive people are those interacting with the data systems in daily basis, because they know the strength and the weakness of the technological protective assets than those interacting with from outside the institution. The ill intended workers who pretend to have the interest of the institution at heart may cause very severe breach, exploit them for their own selfish interests and damage the infrastructures.

Therefore it is important that the institutions should purpose to create awareness to their employees on the information systems security. It will reduce risk of losing data and ensuring effective information systems implementation.

In addition, Stephanou&Dagada (2014) in their study noted the knowhow, behavior and perception of the workers determine the protection and also very critical to any information security programme.

It will lead to effective information systems implementation. Therefore all the workers should follow strictly the specific laid down procedures and practices stipulated by the organization to avoid unnecessary harm occurrences.

The ISO27k Forum (2011) stated that all workers and other outside users of information security control systems should sign a confidentiality agreement. In addition, it further emphasized that any employee, contractor and third party user leaving the organization or moving out of employment the privileges they had when interacting and executing their roles should be disabled and the security related properties returned.

Moreover, a formal disciplinary process should be put in place to be used by all workers committing security threatening actions. Routine system updating practice, the workers and other outside users know how and education of an organization is necessary as they execute specific roles to provide adequate and effective protection required of the security infrastructures,(ISO27k Forum, 2011).Abu-Musa (2007) in Saudi Arabia study he found out lack of security technical knowhow and education brought about harmful operations that exposed the systems to serious threats and breaches. The protection pattern should be mainly concerned with the use of the appropriate framework which would provide adequate protection against the evolving threats and risky issues.

Therefore, the workers technical knowhow and education should be provided in technical learning institutions, so they may easily handle threatening security issues occurrences and to enhance information security controls systems effectiveness within the institutions.

### 2.3.3 Information Security Access Methods

Calder & Watkins (2008), Information Security Access Control (ISAC) is a way of permitting or denying the use of a specific asset by an individual entity. These included Authentication, Authorization and Audit, Specific roles of managing all information security assets should be put in place to allow authorized persons to access the computing resources and information within the organization. Musa (2014) argued that users interacting with network assets strictly need to be properly restricted and only permitting them at different privileges of information access to prohibit and prevent unauthorized entry to sensitive data. There are many methods which would be used to secure the data control systems, which include use of voice password, Iris scan and biometric methods to restrict the data access, providing effective data protection. Stolarski (2012) argued that the reduction of threats facing the institute's data usage may be done by use of enforced intruder's blockages that may prevent direct access to where the data is stored. This physical access control included: the good fit entry points that may offer necessary protection over malicious intruders and hackers. The usage procedures and practices would deter the malicious system crackers and hackers to reach and interfere with the protected data. Stolarski (2012) further highlighted that in order to establish strong information access control methods it is important to provide constant security data experts as far as its protection is concerned. He further said that to have well-coordinated and planned data protection, it's important to use data vaulting techniques which may provide a well secured data protection environment.

Government of Canada (2017) in their Internal Audit Final Report May 2017 stated that purpose of an audit is to check whether the guidelines, procedures and the overall framework has towards the effective control and preventing unauthorized data. The recommended and best standards, practices and procedures used in the audit of the data protection and maintenance.

Hau (2017) stated that to reduce the data threats in an institution and to offer enough data protection from all ill minded and malicious crackers and hackers reaching and tempering with important data within secured control systems, making sure that the people allowed to use the institute data are authorized to do so and also to which specific levels of authorization. All the technological assets for internal processes of the network resources functionality and other types of resources used should have the protective mechanisms put in place to boast data protection within the organizations. Appropriate data protection is commonly determined by the standards and a well written and planned framework, which stipulate good data control environment which provide enhanced and effective data security control systems. The breaches performed by the workers and other people associated in the usage of the data may be reduced by proper establishment of well documented procedures and practices in the organization

In addition, Musa (2014) in his article said that in various technological security assets in an organization control mechanism should be effectively established to have effective data protection.

Data protection and access measures involves well fitted doors, such as well secured strong rooms, processes controls, frequent changes of the passwords, individual administrative controls, and data protection education awareness and training.

Musa (2014) further highlights that appropriate data protection procedures put in place when using it would go a long way in improving data protection in the institution systems. Specifying roles and the responsibilities of the individual employee may help to minimize the threatening issues to the systems since every person would be accountable of their actions. The person responsible of granting the user permission and authorization for instance should be different from one removing users privileges. Procedures such as granting, denying and deleting access to data at various privileges levels are also highly recommended to enhance data protection. Encryption, access denial when the user has three wrong trials, inactivating and putting  the user access dates if the account has not been used for a specified period of time further protect the data. The institutions should ensure at all times that data protective procedures are always updated to prevent unauthorized access.  Remotely accessed data should be strictly done by use of Virtual Private Network (VPN) that would protect from both user communication and authentication. A firewall is required to protect the internal network from external and public networks, hence preventing any an authorized access to the institution data.

### 2.3.4 Information System Environment Practices

The institutions should have well laid procedures and guidelines to boast, promote and counter check the data breaches, this would go a long way to improve the overall data protection in the colleges. The recommended best procedures, standards and guidelines need to be used at all times.

The recommended guidelines and framework should be used concurrently give appropriate required solutions to data protection issues, use of recommended standard gives a framework within which to have a sound security program (Arnason et al., 2008).

The institution system quality would be greatly determined by the best recommended standard, especially the ISO 9001:2015 which is commonly known for the improvement of the systems quality. The implementation of the usage procedures, checking, updating, and improving an organization's information security control system (ISCS) is enhanced by guidelines used.ISO 9001:2015, Code of Practice for Information Security management used to provide direction and data protective environment would be granted properly by the uses of the best recommended procedures and guidelines, hence reducing data breaches drastically.

Good implementation framework has data security procedure which is grouped into four levels and layers procedures of foundation, procedures of establishment, procedures of providing the assets and procedures of checking and auditing. The procedures of upgrading and maintenance are good security practices of enhancing data reliability and protection in the institutions.

The recommended best procedures and guidelines are used to facilitate the institution activities. Continuous checking, monitoring and auditing is a method to ensure the systems are always effective in managing the protection of data, hence reducing the evolving complex security threats in the institutions.

Usage of effective data protective procedures and guidelines help to handle and comprehend how to improve on tactics to maintain and protect the data against the increasing data breaches of the institute at all data protection levels. Checking, verification and auditing enhances effective data protection, frequent monitoring and evaluation of data protective devices may promote better functionality and activities of the institution.

Effective data protection and control would promote the flow of high quality and reliable data in the institution.

(Radack, 2011) stated that data protection using the recommended procedures , guidelines and a good framework make the institution achieve its purpose when working with well protected data, providing data of high quality  and reliability in the institutions.

Chaulaa, Yngströmb&Kowalskic (2017) viewed Evaluation of data protection as a method of checking, monitoring, evaluation and auditing of the laid down security procedures, guidelines and standards governing and maintaining the data security control systems. This provides an assurance and facilitates enhanced data protection, quality and reliability against the data breaches in the security systems used in the institutions.  This process is known as data protection assurance. Data protection is very demanding in terms of time consumption and expenses due to the involvement of the expensive technological assets and resources, education and training of personal, procedures and guidelines used to accomplish it.Data auditing and monitoring group help the institution to have constant review and assurance of well protected data security systems at all times. The auditing, monitoring and evaluation group helps an organization in mitigating security risks and during audit process it covers institutions procedures, guidelines and practices rolled out and used in daily basis when executing various roles. The auditing, monitoring and evaluation group assesses the procedures, guidelines, practices and policies and whether they are protective enough to all institution operations and the ability to accomplish the aims of the institution fully. (RMAS, 2017) stated that this auditing is directed and governed by the use of international recommended and accepted standards to improve and perfect the data protection in the institutions. Steinbart et al. (2012) investigated four institutions and found out that improved.

Data protection is determined by the cooperation between the employees and the auditing, monitoring and evaluation group. The importance of this cooperation promotes the approval and acceptance of various data protection processes by stakeholders within the institution.

(Steinbart et al. 2012)stated that the audit report and analysis would be utilized by the data protection expert involved in maintaining the data security systems to improve them even further to enjoy continuous and appropriate data security and control.

(Steinbart et al. 2013) conducted an investigation of data protection experts from several companies and indicated that the cooperation between the audit and the data protection enhancement, promotion, motivation and change of their altitudes concerning total data protection control in the institution.

## 2.4Information Security Control Systems in Kenya Colleges

(Laudon, 2012) stated that data protection against issues and threats experienced by most Kenyan technical college institutions.

Data protection is involved with the process of improving security control systems to enable them to handle continuous and evolving complex and difficult data threatening issues to enhance data quality and reliability.

The data security control systems that are easily compromised and suffer damage and various form of data attack is a clear indication they lack full and effective data protection control in the institution. A successful attack on information security control systems signifies that it is highly prone to these attacks (Alahboul, 2010).

(Salmela, 2008)stated that data protection procedures, guidelines, practices and standards are the most important recommended to control and provide appropriate and effective data protection within the network  resources in the institution.

The institutions of higher learning are required to offer the necessary protection of all data in their institution without alteration, compromise and loss of the same. These institutions of higher learning need to provide continuous protection of the data in the security control systems always without any compromise.

(Solms, 2009) in his study indicated that the recommended procedures, guidelines and standards are very important in offering effective data protection, The users with low education and technical knowhow to comprehend and handle the data threats have contributed greatly towards the data security control compromise within the institution systems. Data threats and issues emerge where the data protection is not fully and effectively achieved and implemented to prevent the use of important data (Kraemer and Carayan, 2007).

Data threats and intrusion by different stakeholders outside the institution who are ill motivated and malicious hack the data security control systems harming, corrupting and accessing sensitive and private data. Data threatening issues analysis report (2013)recorded that the former or active employees and other people who had previous interacted or are interacting with the institution protective control systems poses a very serious threat to data protection within the organization. Malicious and ill motivated employee and other stake holder interacting with these systems must plan to attack them to access the important and sensitive data of the institution; alternatively it may be as a result of lack of technical knowhow and awareness training.

Complex data threatening issues have emerged, evolved and have continually increased recently, hence calling for drastic and more cautious data protective measures against this trends that are changing in daily basis. Lot of expenses in terms of millions of pounds and dollars are spent to curb the increasing data threats and fraud activities faced by various institution frequently as indicated by (Gupta & Sherman, 2012.All the institutions big or small are equally facing data security threatening issues that corrupt and cripple down various important operations pertaining these according to (Security breaches survey, 2013). Institutions of higher learning are also facing data threats when using the systems when performing various tasks of the institution where data is not effectively protected. Kenyan institutions of higher learning in the recent past have faced the highest data fraud and attacks among the African institutions noted by information security service provider Cyberoam (2015).

Many data security breaches have been recorded in African institutions, but Kenya is the first followed by Egypt, Morocco, lastly South Africa. Education institutions are actually being targeted a lot, grades and fees alteration and also manipulation has been witnessed done by selfish and ill motivated people. Many criminals are making huge amount of money from these activities especially before the exams results are out and at beginning of the terms during fees payments within the institution.

(Information security service provider Cyberoam (2015)noted that appropriate and effective data protection should be accorded to important and sensitive data against the continuous emerging data threat facing the institutions especially Cybercrimes. Trainers and lecturers have suffered data threats from the very own learners the have taught and acquired more computer skills using them to attack and hack their systems.

In 2011, very serious damage and attack was experienced in the Kenyan police data protective control systems at the late hours of the night, where attacked and harmful emails were hauled and posted, which was a very ugly experience.

The users interacting with the data protective devices have little technical knowhow and education to protect the data threats and attacks. This has caused the institutes data security control systems to be hacked and important data accessed, also tricked by malicious and ill intended people to expose the institute sensitive and private data.

The technical college institutes have continued to suffer increased attacks of their private and important data affecting their operations and their daily activities, also big losses within the institutions.

The greatest losses are from ignorant workers who are not conscious of the danger facing and threatening the institution data, due to low level of technical knowhow to protect the data. Many criminal hacking activities are happening every now and then because the hackers of the systems device new ways of the attack, some of these cases are reported others are not.

According to Kenya Cyber Security Report (2017) the institution should up their game of protecting their data by use of recommended procedures and guidelines, frequent audit and monitoring as well as educating the users on data protection awareness meant to provide effective data security control.

## 2.5 Review of Related Studies

This section presents the related literature and studies on the effective information security control systems after thorough and in-depth search that was done by the researchers.

### 2.5.1 Information Security Control Systems in Kenyan Technical Institutes.

Hau (2017) stated that the use of stipulated security data procedures and practices would facilitate and avoid important data alteration and invasion by unauthorized users, hence reducing frequent data attacks The institution all operations and processes should be well protected at all times, the data protective devices checked, audited and monitored frequently to reduce the data threats and breaches, which enhance and improve the data protection. Effective data protection involve well-structured implementation framework consisting of procedures, guidelines and practices that would provide good data protective environment of the important data.

Whitman and Mattord (2008) stated that there various types of data breaches and issues, some occur due to the low level of user's knowhow, others due to ill motivated and selfish actions , ignorance of the workers, existence of hackers who use the disclosed information to them and also internal network attacks all of them become the source of data compromise. The greatest threats and attacks experienced in the institutions are from the ignorant ill motivated and malicious works of these institutions (D'Arcy &Hovav, 2009).

The data protective experts and the users need frequent change of protective techniques. Emerging data non protective issues would result to data breaches data alteration and attacks.(Johnson, 2008). According to Kumar, el at, (2008), The data breaches are as result of exposed data protective technological assets to hackers and crackers of these systems ,who always device new ways and techniques of the attacks.

Continuing global threatening issues to data protective devices to be vigilant and extremely conscious of data threatening issues view (Calder and Watkins, 2008). To ensure these issues are contained, many information security standards and framework have been put in place.

Many governments and organizations have come up with functioning bodies for creating benchmarks, guidelines and practices to promote effective data control by implementing the appropriate techniques and framework to improve quality and reliability of data in the institution.

This implies that the study on effectiveness of an information security control and practices cannot be exhausted without considering administrative support, environmental factors and the availability of resources. Various standards, procedures, practices and guidelines used internationally to audit, monitor, secure and protect the technological assets in the institution.

### 2.5.2 Layered Defense Security Strategy

(Tipton and Krause, 2000) stated that the principle provide layered security which would enhance the security of the whole system. Data protection would occur through the use of different levels of data protection of which if an attack would not pass through one layer it might not pass the rest of the layers. This technique would help to reduce the risk posed to information security control systems. Security policies should be the backbone of information security control plan. Policies are used to protect technological information assets, using the recommended practices. Policies implementation effectiveness is determined by the way they are communicated promoted and enforced. Policies and the necessary standards and guidelines are implemented by using procedures which provides details on how to implement them to have good data protection within the institution data security control systems. Technical knowhow and education concerning the data protection would be important of the people interacting with the data to facilitate its protection. They should also know security related practices, processes and the result of a security threatening issues. Layer two is physical security used to restrict unauthorized people to access information technology assets.

Layer three is perimeter security layer, which direct where traffic to go through from the outside (untrusted) network to the inside (trusted) network. Network Firewall is the most important to ensure effective information security control system.

Layer four focuses on internal network security control protecting the corporate IT assets. Layer five is host layer which facilitate all network flow using a device to connect the source and the destination. Workstations, servers, phones and other mobile devices are some of the destination devices used. Anti-virus is a very useful software device of host layered security; the use of this software would provide the necessary data protection in all data flow usage devices.

Layer six deals with Software applications which are commonly used in the institutions to execute daily activities, which may be easily attacked.

Last level of data protection is meant to protect the important and sensitive data itself. Protection methods and techniques used at this level are concerned to safeguard and offer the best data protection within the institution.

### 2.5.3 Standards and Frameworks for Information Security Management Theory

Appropriate data protection would be improved by frequent checking, monitoring and auditing of the data control systems of all the procedures and practices used in all processes and devices. ISO 9001:2015, ISO 9001:2008, and NIST 800 series have been commonly used.

Even if there is no one security standard that may give all the solutions to information security requirements, a recommended standard may give a framework to provide effective and proper data protection in the technical colleges.(Arnason et al., 2008).

The ISO 9001:2015is a mandatory requirement international standard for best data protection that would be used to ensure data is effectively protected. It would improve especially on data quality and reliability.

The use of various recommended procedures, guidelines and practices in all college processes and devices would go a long way to offer a lasting solution of data protection.

The technical knowhow and education of appropriate data protection would be generated from the recommended and best guidelines commonly used to provide the necessary data flow protection and business continuity management.

This Code of Practice is the best to offer effective data protection.IT Governance Institute (ITGI) 1992 stated that the recommended data protection procedures guidelines and practices provide the best data protection in all processes used within the institutions.

COBITIT processes provide a basis for establishing and maintaining good security tasks. It has become one of the best used frameworks globally to offer enough data protection in all the institutions.

### 2.5.4 Information Security Management Best Practices

Peltier et al. (2005) stated that good foundation of appropriate data protection is well documented procedures and guidelines. These procedures and practices when used properly they prohibit greatly the planned threats and attacks of the data within the various operations and processes of the institution.(NIST, 2003) stated that the recommended procedures, practices and guidelines need to be very specific and narrowed down to the institution requirements which would be a good base to curb the data threats and breaches, hence realizing the institutes goals and objectives.

Another very fundamental practice of a good information security program is to ensure proper user's education awareness and training. (Arnason and Willet 2008) stated that technical knowhow and education increase is very important and requires frequent upgrading. Data functions and specific work should be properly stipulated for individual worker during employment, in case of data breaches they can be narrowed down to that person. An institution should also ensure first time employees are properly oriented for information and information technology asset security mechanisms. Which help the workers to deal with who violate the laid down procedures and practices, compromising the data protection in the institution Calder and Watkins, 2008). Data checking monitoring and audit is very important for data protection and control. National Institute of Standards and Technology (1995), stated that to  boast data protection at all times, then data audit and evaluation is required and (Arnason and Willet, 2008)  also concur and agree totally with the same sentiments The best way to deal with data threats always is to follow strictly the laid down procedures and continuously updated.

The ISO 9001:2015 is a necessary standard to ensure that the physical and environmental information security control is good (ISO27k Forum, 2011).  Physical handles would be required to bar the intruders to invade and attack important information security control facilities.

(NIST, 2003) stated that data security threats are not easy to foresee hence an institution should be well placed to handle data security issues by frequent checking, monitoring and auditing data protective devices against continuous evolving complex data attacks .This would guarantee the data threatening issues and occurrences facing the data systems are communicated in such a way that proper action is taken.

Threat processes procedures can ensure the certainty to respond very fast and appropriately to interferences of services.  (Calder and Watkins, 2008).

Access control is where a user is permitted or denied the use of a specific information asset depending on access levels. Data protection involves prevention of interaction and access of private and sensitive data without any permission of necessary authority(Calder and Watkins, 2008) stated that establishment of the processes and practices of information security control within data protective assets may be very crucial.

For smooth running of daily processes to occur, then data protection procedures and guidelines are paramount, which enhances business continuous of the institution.

Information security control systems effective working would be determined by proper audit, monitoring and evaluation frequently (Calder and Watkins, 2008).He further stated that Managers should make sure data protection and control practices stipulated in various processes need strict follow up and evaluation to fulfill the college objectives and purpose.

## 2.6 Summary

Technical, Vocational and Education training institutes should be adequately prepared to understand what information security infrastructures they have, and ensuring their security is appropriately done. Deloitte East Africa (2011) stated that the employees pose a higher security threat in comparison with those from outside East African Organizations. The use of various recommended procedures, guidelines and practices in all college processes and devices would go a long way to offer a lasting solution of data protection.

# CHAPTER THREE

## 3.0 RESEARCH METHODOLOGY

### 3.1 Introduction

This chapter presents the research methodology used in the study. The chapter introduces the research design, where the study was conducted, the target population, the population sample, the research instrument and how to make the instrument valid and reliable. The chapter also states the data collection method, data analysis method and presentation of the results that were used in the study.

### 3.2 Research Design

Vaishnavi & Kuechler (2004) stated that a research design is the detailed documentation of plans and processes for research assessment and investigation of data security control. Creswell & Plano (2009) stated that a research design involve the description, inference and relationship of the research variables, that is plans and processes for research that emerge from wide assumptions to well explained detailed assessment and comparison of independent variables and dependent variable .

The descriptive survey research design, because it helped to investigate information security controls systems and related data protective management practices in Technical Training Institutes. The descriptive survey design is ideal since it contribute in assessment of the inference and relationship of the four independent variables and the dependent variable in a research study (Edwards, 2006).

Descriptive survey describes accurate description of people perceptions and the detailed information security control practices utilized in college institutions.

However, to successfully achieve the goals of the research, the researcher utilized both qualitative data as well as quantitative data techniques. (Mugenda and Mugenda 2003) stated that a detailed descriptive research technique provide proper investigation and accurate results and conclusions

### 3.3 Target Population

All respondents to be used in the research study formulate the people included in the research (Marczyk, DeMatteo and Festinger, 2005). Israel (2012) noted that the target people are those to be used in the research data collection and analysis. The study population consisted of all Technical Training Institutes in Nairobi County. There are 20 recognized Technical Training Institutes in Nairobi County according to the Commission of Higher Education. The sample security experts groups included ICT managers, IT workers, system controllers and Network controllers, ICT maintainers and ICT support worker collectively, known as data experts who control and provide the best data protection in the technical college institutes.

**Table 3.1: Category of Colleges, Number of Colleges, Number of ICT Security Experts**

| College category | Number of college | Number of ICT security experts |
|---|---|---|
| Public college | 8 | 268 |
| Private college | 12 | 446 |
| Total | 20 | 714 |

### 3.4 Research Sampling Technique and Sample Size

Population involved in the data collection is the selected number from the rest of the whole target number of people (Marczyk et al, 2005) When selecting Technical Training Institutes in Nairobi County to be used in this study Probability sampling technique was used. When using probability sampling method any of the selected objects has an equal chance to selected (kothari, 2004).

### 3.4.1 Sampling Techniques

The objects of the population that the researcher wishes to involve in his study consist of a complete list of all sampling frame.(Turner, 2003)stated that the objects selected for the research data collection to provide the specific objects to be involved is generated from sampling frame. The object size is specific number involved in data collection out of all the number which will be used in the research study. Sampling is a method of getting and choosing the objects to be involved in this research study data collection.

Involving a big number of objects may result in high magnitude of data collection and analysis; the higher the number involved the higher the chance of errors rise (Israel, 2012).

The detailed description of the objects used should be the same of the entire number of all objects.(Nyaboga, 2011).Israel (2012) stated that to choose the objects to be involved in the research study categorised random choosing method was the best method. The ICT security Expects were stratified depending on the type of Technical Institute in Nairobi County as categorized by theCommission of Higher Education as either public or private technical training institute.

To identify the particular ICT security Expects in each stratum to participate in the research study the researcher used a purposeful sampling technique. To handpick respondents who were relevant to the research questions the researcher used random purposeful sampling technique because it’s not based on advanced knowledge of how the outcomes would appear and to increase credibility not to foster representativeness The sample was composed of a purposeful random selection of 30% of college, ICT security Experts respondents to represent entire group from various public and private college in Nairobi County.

### 3.4.2 Sample Frame

According to Mugenda and Mugenda (2003) 10% -30% of total population forms a representative sample; the researcher should take as big a sample as possible if researcher has adequate time for the study to ensure that someone else would get similar findings to a higher degree if he/she selected another sample of the same size. In this research a sample of 30% of Technical Training Institutes Nairobi County was randomly selected to represent the sample.

Six out of the 20 Technical Training Institutes in Nairobi County were selected randomly; this enabled research to handpicked Technical Training Institutes with more advance security software’s and practices.

The sample included Nairobi Technical Training Institute (NTTI), and Zetech College (ZTI), Kenya School of Monetary Studies (KSMS), Nairobi Technical and business studies (NIBS), Railway Training Institute (RTI) and Graffin's College (GCK)

The researcher chooses the number of objects from strata/subgroups of security experts through the categorization random sampling method. In this method, the objects are grouped into a number of non-repeated subgroups or strata or selected items are from every group (Kothari, 2004). From the chosen Colleges the objects were chosen from each of the subgroups randomly. A random purposeful sampling technique was used to handpick respondents and colleges believed with relevant information about information security management systems.

**Table 3.2 Category of Colleges, Sample Size of ICT Security Experts**

| **Colleges category** | **sample size of college** | **Sample size of ICT security Experts** |
|---|---|---|
| Public college | 2 | 81 |
| Private college | 4 | 135 |
| Total | 6 | 216 |

### 3.5 Data Collection

The use of questionnaire was the main method of data collection in this research. The researcher developed questionnaires for security professionals of data security. To come up with the questionnaires technical knowhow and their education was considered .The respondents received the questionnaires personally or via email in some institutions.

According to Ogila (2002), a questionnaire is a carefully designed instrument, written and typed or printed for collecting data from people. Well written detailed questions used by the selected group to give responses about themselves and any other response required in the research (Sivo et al., 2006). The questions contained in the questionnaires followed a definite order for to guide the respondents.

The respondents were expected to read and understand the questions and write down the responses in the spaces meant for that purpose in the questionnaire itself. This method has a large coverage enabling the gathering of data from a large sample very convenient and inexpensive. It also has anonymity which helps the researcher to collect more accurate answers than is possible in an interview. Mailing questionnaire for the data collection is not expensive even when collecting huge volume of data and widely distributed compared with other methods. The selected individuals provide biased free answers from the interviewers due to enough time provision (Kothari, 2004).

## 3.6 Validity and Reliability

Validity is termed as an indication of the device is appropriate to measure correctly what is required to measure (Kothari, 2004). Pilot study was done first in this research, which confirmed questionnaire ability to succeed in collecting the correct data. Before the pilots stage the checking and discussion was done by the supervisor, which aimed and purposed was to facilitate an improved data collection device.

### 3.6.1 Pre-test of Research Instruments

The validity and reliability of the instruments was done through a Pre-test study in this study. Jordan private college and Thika technical public college not included in the main study of this research in the pre-test.

The supervisors gave the researcher advice in order to minimize the instrument’s error found in the research instrument evaluation; the researcher sought expert advice from in the evaluation of the instrument.

The feedback from the experts assisted in the development of a valid research instrument. The device’ validity was updated through evaluation and review. The researcher administered the research questionnaires to these respondents randomly. The Pre-test study helped to improve the overall highly correct and content of device.

### 3.6.2 Reliability of Research Instruments

A reliable measurement is that which when  an instrument gives same analyzed data if repeated a several it’s considered a reliable instrument as it did the first Kappa time. When the results are different when repeated several times it’s an indication that it’s unreliable (Mugenda, 2008).

A research instrument that yields consistent same results or data over and over again or many trials (Mugenda and Mugenda, 2008) is an indication that it’s a reliable measurement. Accurately and consistently variable measurement obtained is the same is a clear indication that the instrument is reliable and obtains the same results under the same conditions.

The researcher made the research instrument as clear as possible by pretesting it using a group of ICT security Expects with characteristics similar to those of the study group, but did not participate in the actual study. ICT security expects from each strata was selected to participate in the pretesting exercise a sign of reliability.

Testing the reliability of the instruments split half method was used. This technique of assessing reliability requires only one testing session.

Cronbach's alpha tested the pilot results. The statistics reflected α value = 0.768, an indication that the questionnaire used in this research study was reliable. The entire validation process assisted in guaranteeing accurate results and as a result a credible research.

### 3.7 Research Data Collection Procedure

The National Council of Science Technology Innovation and Kisii University, Nairobi campus permitted the researcher to conduct the data from various institutions .These letters acted as an introduction of the research topic. It was handed over to all the relevant authorities who were directors of ICT, IT security staff, system administrators and Network administrators and ICT users support collectively known as ICT security experts of information systems.

### 3.8 Data Analysis

Quantitative and qualitative data were both generated in this study. Descriptive statistics was used for data analysis according to the research study objectives and questions. The analyzes of data was done using SPSS (Statistical Package for the Social Sciences) version 20 to arrive at mainly means, standard deviations, frequencies and percentages.

Graphs and tables were also used to represent the findings.Interpretation and drawing up of conclusions and recommendations were done through the calculation of percentages for each response Cooper and Schindler (2003) further noted that the two benefits associated with the use of percentages, one is data simplification through limiting all the number to range between 0 and 100, also to translate the data into standard form with a base of 100 for relative comparisons.

## 3.9 Ethical Considerations

Blumberg et al., (2005) defines ethics is concerned with the perceptions, norms, the culture, the behavior and how individuals respect themselves. Since this study was requiring the involvement of individual reaction, various behavior and negative perception were tackled. These ethical issues needed to be considered for the purpose of ascertaining the privacy of all the respondents.

In this research study process the most important ethical issues considered was the consent and confidentiality of the respondents. The study was carried out with utmost ethics. First, before the respondents were handed the questionnaires, the researcher sufficiently briefed them on the purpose of the study so that they could participate at their own consent.

The data collected was used for the purpose of the study only, therefore respect, confidentiality and privacy of the respondent personal data was accorded. Lastly, it is only the data collected for the purpose of the study which was presented as the findings without any fabrication of the results.

# CHAPTER FOUR

## 4.0 DATA PRESENTATION, ANALSYSIS AND DISCUSSIONS

### 4.1 Introduction

Analysis and findings of the study are presented at this chapter .The investigation done this study was on the policies affecting effective information security control systems in public and private colleges in Technical Training Institutes in Nairobi County.

It consists of the following Sub-topics: questionnaire return rate, data demographic information of the respondents, information systems environment practices adaption, diffusion of security access controls, current existing security policies of information security control systems, the impact of security awareness in public and private colleges, recommendations and conclusion for policies affecting effective security control systems.

The findings are based on data collected using questionnaires from the information security experts in Technical Training Institutes in Nairobi County.

### 4.2 Response Rate

The study was conducted in six Technical Training institutes in Nairobi County. The researcher administered questionnaires to 216 ICT information security experts. The researcher collected the questionnaire from the respondents after completion.

The response rate of respondents was issued to give the details of collected data. Out of 216 questionnaires distributed 153 were appropriately filled and returned. For the analysis of this research study a return of 153 (71.5%) was good and recommendable**.**

### 4.3 Respondents Characteristics and college categorization

The respondents are the ICT experts in the Technical Colleges and the categories are based on both the public and private Technical colleges.

### 4.4 ICT Security Experts Response on Types of Technical Training Institutes Categories

Type of college is important in establishing the various policies that influenced effective security control systems in selected Technical Training Institutes in Nairobi County. The type of college category was provided by ICT security experts. The findings show that 105**(**68.6%**)** ICT security expert's respondents were from private college. Private security experts were many because private colleges have a mixture of different setting this included: pre-university, technical and Satellite Campus settings this forces them to have many security experts 'workforces to safeguard technological assets in these institutions.

**Table 4.1 ICT Security Expert's Response on Types of College Categories**

| ICT experts response college categories | Sample ICT Experts | Responses | Percent |
|---|---|---|---|
| Public College | 81 | 48 | 31.4 |
| Private college | 135 | 105 | 68.6 |
| Total | 216 | 153 | 100.0 |

### 4.5 To determine how college security policies affect effective Information security control systems in Technical Training Institutes in Nairobi County.

A total of 153 number of ICT security experts were to give they views on the various statements about the security policies that were affecting effective Information security control systems in Technical Training Institutes in Nairobi County.

According to (Peltier et al., 2005), a security policy is composed of rules and regulations used to control the unauthorized use of the institution assets to ensure high data security control and privacy. According to (Box &Pottas, 2013) argued that employees' technical knowhow and altitude of data protection, privacy and practices influences data protection control behavior and the data protection control and privacy patterns.

The following were various research responses, 78(51%) of the respondents were in agreement there were no extent control systems proper implementation of government security policies. Only 24(15.7%) strongly agreed there were large extent of proper implementation of government security control systems policies in their respective colleges.60 (39.2%) with no extent respondents were in agreement that there were little or none of colleges security systems control policies, while 9 (5.9%) agreed there were large extent of security systems policies which in turn enhanced systems reliability in their respective colleges.

Bulgurcu et al., (2010) approved and asserted this statement that in the presence of information security policy culture; it helps to enhance the information security and a place where data highly secured from hackers and malicious users who have bad intentions and altitude. He further emphasized that employee's awareness on information security rules and regulations results to better attitude towards it, which reduces harmful security behavior (Parsons et al., 2014).

**Table 4.2 Security policies affecting effective Information security control system(N=153)**

| Level Agreement | Large Extent % | Medium Extent % | Undecided % | Little Extent % | No Extent % | Total % |
|---|---|---|---|---|---|---|
| Variables | | | | | | |
| Extent of Government Policies | 15.7 | 6 | 17.6 | 9.8 | 51 | 100 |
| Extent of college Policies Implementation | 5.9 | 11.1 | 9.7 | 19.2 | 39.2 | 100 |
| Proper Implementation of Security Systems Policies will enhance System Reliability | 33.3 | 17.2 | 8.6 | 13.8 | 21.6 | 100 |

### 4.6 To establish the security awareness impact on effective Information security control systems in Nairobi Technical Training Institutes.

A total of 153ICT security expert's respondents were required to indicate the impact on security awareness affecting effective Information security control systems in Nairobi Technical Training Institutes. The table 4.3 shows that there are no well-trained end users that would influence the effective security control systems.

The findings of this study are in agreement with the findings of Arnason& Willet (2008), stated that employees must be informed of security problems and how to maintain it. The management should ensure that security specific functions of the employees are well indicated in the set working conditions and terms of employment. 72(47.0 %,) of the respondents were in disagreement that colleges had well trained end users that influenced effective security control systems in Technical Training Institutes in Nairobi county.

Only 24(13.8%) of respondents agreed that colleges had well trained end users that influenced effective security control systems. Moreover, Calder & Watkins (2008) highlighted that an organization should carry out employee orientation about information and information technology security and also developing and enacting legal disciplinary rules for workers committing security crimes. Only33(26.6%)of respondents were strongly in agreement that their colleges had well trained end users influenced effective security control systems in Technical Training Institutes in Nairobi county.84(54.9%) of respondents strongly disagreed that there had security control systems users' support personnel for security control systems in public and private colleges, and only 30 (19.6%) strongly agreed. Lack of enough security control systems' support personnel was a great hindrance to enhance effective security control systems. 60(43.0) disagreed that there had integrated and adapted security control systems confidentiality agreement which was fully used and utilized in the day to day college management activities in Technical Training Institutes, while 30 (19.6%) strongly agreed that college have integrated and adapted security control systems confidentiality agreement. 57 (37.3%) of respondents were in disagreement that colleges management had well-functioning security control systems disciplinary procedures for security control systems, only 27(17.6%) strongly agreed that college management staff have adapted security control systems disciplinary procedures for security control systems.

According to Stephanou&Dagada, (2014) stated that in their study on the information security awareness training on information security behavior was critical to any information security programme. Also it will lead to effective information systems implementation, therefore awareness of policies is needed by all individuals in an organization to ensure that policies are well understood and not misinterpreted.

The findings therefore indicate that there was lack of adequate security awareness and training of security control systems that was affecting effective security control systems in public and private colleges in Nairobi County.

**Table 4.3 Impacts on security awareness affecting effective Information security control systems(N=153)**

| Variables | Strongly Disagree | Disagree | Undecided | Agree | Strongly Agree | TOTAL |
|---|---|---|---|---|---|---|
| Level agreement | % | % | % | % | % | % |
| Trained users Influenced Security systems | 47.0 | 9.8 | 5.9 | 15.7 | 21.6 | 100.0 |
| Hard Security Users' support Personnel | 54.9 | 11.8 | 1.9 | 11.8 | 19.6 | 100.0 |
| Security Control Confidentiality Agree Utilized | 39.2 | 3.9 | 5.9 | 31.4 | 19.6 | 100.0 |
| Hard Security Disciplinary Procedures | 37.3 | 9.8 | 13.7 | 21.6 | 17.6 | 100.0 |

### 4.7 To examine how the information security access methods affect effective Information security control systems in Technical Training Institutes in Nairobi County.

A total of 153 ICT security experts respondents were required to rate their agreement with the various statements about the information security access methods that were affecting information security control systems in public and private colleges in Nairobi County. 105(68.6%) of the respondents were in disagreement that colleges had adapted user' registration procedure plan for security control systems in teaching practices, while 33(21.6%) strongly agreed with the statement.

These findings were in agreement with the findings of Musa (2014) argued that to have control of individual access to private data. Further indicated that permission to access any data assets and infrastructures of the institution must follow strictly the stipulated practices set to ensure data is properly protected from hackers and ill motivated users.

36(23.5%) of respondents were in disagreement that their colleges have Integrated and adapted security control systems access right reviews management. Only 30 (19.6%) agreed that there Integrated and adapted security control systems access right reviews management.

33(21.6%) of respondents were in disagreement that Institution management staff has segregation of duties for information security control systems, while 90(58.8%) strongly agreed on staff duties segregation which enhanced effective information security control security systems in Technical Training Institutes in Nairobi.Musa (2014), indicated that the best practice may include the concept of least privilege, which ensures granting users the right level of privileges.

If a person needs to read a file, then there is no need to grant them delete access. Paraphrases, locking accounts after three invalid attempts, disabling unused accounts and setting expiration dates on accounts are also good security practices. Moreover, universities are encouraged to limit remote access to their resources.

If they have to allow remote access, it should be done through a Virtual Private Network (VPN) with two-factor authentication required. Furthermore, publicly accessible content would need to be physically and/or logically separated from the internal network by placing them in front of the firewall, an area commonly known as the demilitarized zone (DMZ) according to (Musa, 2014).

**Table4.4Information security access control methods affecting effective security control system(N=153)**

| **Variables** | Strongly disagree | Disagree | Undecided | Agree | Strongly Agree | Total |
|---|---|---|---|---|---|---|
| **Level agreement** | **%** | **%** | **%** | **%** | **%** | **%** |
| Adapted Registration User procedure plan | 56.9 | 1.9 | 5.9 | 13.7 | 21.6 | 100 |
| Integrated access Security Right Management | 23.5 | 15.7 | 11.8 | 29.4 | 19.6 | 100 |
| Institution Management Staff has Duties Information Security Control Systems | 21.6 | 11.8 | 5.9 | 1.9 | 58.8 | 100 |

**4.7.1 Number of information security control systems Technical Training Institutes have adopted for effective security control in Technical Training Institutes in Nairobi County.**

A total of 153 ICT security experts respondents were required to rate their agreement to the information security control systems stated factors in line with control security systems. Majority of the respondents reported that effective implementation of the current information security controls and industry best practices in information security control was low with most responding that effective implementation of security control systems were No extent. Concerning clearly stated security control specific functions of all employees in stipulated conditions and terms of employment in security control systems effectiveness in institutions.

### 4.8 To establish how Information system environment practices affect effective Information security control systems in Technical Training Institutes in Nairobi County.

A total of 153 ICT security experts respondents were required to rate their agreement with the various statements about the information system environment practices affecting effective Information security control systems in public and private colleges in Nairobi County.

According to Government of Canada (2017) in their Internal Audit Final Report May 2017 stated that purpose of an audit is to validate the practices and guidelines put in place to ensure that the institution data is highly protected to prevent hacking and malicious attacks from both the employees and other users of data access control systems.

The auditing and validation methods need to follow stipulated and recommended practices and guidelines to provide proper data privacy and protection within the institution.

75(49.0%) of the respondents were in disagreement that colleges had adopted recommended ISO standards for effective security control systems in their college.

27(17.7%) strongly agreed with the statement by ( Steinbart et al. 2013) that previous research done on ICT experts in many organizations found out that proper data protection ,internal audit and validation process may lead to improve the altitude of the ICT data protection officers, which eventually result to high and appropriate data protection within the institutions.42(27.5%) of respondents were in disagreement that their colleges having monitoring of security control systems will improve reliability of services delivery, while 54 (35.5%) agreed that the monitoring of security control systems will improve reliability of services delivery. 36(23.5%) of respondents were in disagreement that security control audit will enhance quality of information for information security control systems.66(43.1%) strongly agreed security control audit will enhance quality of information which enhanced information security control security systems in Technical Training Institutes in Nairobi. Many frameworks and recommended practice guidelines are there in the institutions to deal with potential data threats , apply and strengthen data protective devices, making use of all set ISO standards pertaining data privacy and protection ,also facilitating data protective rules have been implemented, no one recommended security framework would solve all problems related to data protection issues within the institution,

**Table 4.5 Information system environment practices affecting effective Information security control system(N=153)**

| Variables | Strongly Disagree | Disagree | Undecided | Agree | Strongly Agree | TOTAL |
|---|---|---|---|---|---|---|
| **Level agreement** | % | % | % | % | % | % |
| Adopted recommended ISO standards | 49.0 | 3.9 | 9.8 | 19.6 | 17.7 | 100 |

| | | | | | | |
|---|---|---|---|---|---|---|
| Monitoring Security Systems Will improve service Delivery | 27.5 | 9.8 | 1.9 | 35.3 | 25.5 | 100 |
| Security Audit Will enhance Quality Information | 23.5 | 3.9 | 1.9 | 27.5 | 43.1 | 100 |

### 4.9 Have security control systems evaluation done in teaching and learning in public and private colleges

The respondents were required to rate their agreement to the diffusion of security control systems in line with Information security systems security. Majority of the respondents reported that diffusion of the security strategy and policies were low. Concerning Effective process to ensure good security practices were poor which attributed to 78.4% reported a great extent, while 21.6% reported low extent, this Implies that most Technical Training Institutes have low or No extent effective process to ensure good security practices, on formal user registration and deregistration system and awareness training for all information systems users as shown in the table 4.6 below.

**Table 4.6 Security Control Systems Evaluation in Teaching and Learning(N=153)**

| **Extent** | **Frequency** | **Percent** |
|---|---|---|
| Great extent | 120 | 78.4 |
| Little extent | 33 | 21.6 |
| Total | 153 | 100.0 |

## 4.10 Proposed implementation Framework of Monitoring End- User Security Policy Compliance

### Introduction

Successful implementation of an effective information security policy shall be determined greatly by the response to user behavior. The author has proposed a framework guided by the collected and analyzed data, that purpose to increase the control level of usage by checking and weighing their behavior. This framework is supposed to give a whole increase level of control of all users, for the purpose of controlling, weighing and monitoring to users' behavior with a data security policy. Also, counting number system (control number system) is used to apply other polices for the suggested framework.

The purpose of utilizing the control number system is to ensure users to be agreeable with the policy, as well as ensuring their agreeing rate with the data policy or any element of it. By utilizing this framework, every item of the data policy is checked which gives institutions a firm idea for their data regulations. An institution is able to know the item of its rule has low or high number of abuses that have occurred for a specific period of time.

This framework for checking the usage data policy agreement for mitigating the problem of non-agreement for data security policies, by frequently checking the usage behavior in connection with data policies and helping institutions in improving agreement levels of their usage. The framework should be customized to fit the institution's operations which is different from various institutions. The most important of the proposed framework is meant to improve the usage awareness of the benefit of proper data security policies usage.

To increase the efficacy of their awareness inputs the users should frequently be subjected to purposed awareness and checking their proper usage of data security regulations. The importance of this framework will be determined by three significant things: checking, usage taxonomy and usage agreement numbers system. To increase the awareness and royalty of end-users it is necessary to use these aspects. The proposed framework contains full information pertaining this framework of effectively checking the behavior usage using agreed numbers system, and to explain and show how the framework should be done.

### 4.10.1 Information Security Policies and Monitoring User Behavior

This proposed framework has two major points: data security policy and behavior of operators (checking operator’s behavior).

### 4.10.2 Data Security Regulations

Data regulation is explained as ‘documented report which explains the right and wrong behavior of usage by users in accordance with how they handle the data technological infrastructure well secured way (Disterer 2013). Data usage for people need be made aware of the minimal available data policy that is in their institutions. Usage regulation acceptability, data regulation confidentiality, regulations for email, regulation for password, regulation for clean desk, regulation for internet usage and regulation for physical access are some examples of data security policy. Every type or group of data security policy has various items (known as numbers items), these are number of reports where every items explain specific thing or behavior that all users should follow. For instance, Table 4.7 has 4 elements from various groups of data policies (SANS 2014).The items of the data security policies in Table 4.7 in the proposed framework are used as examples to show how it working process occurs.

The suggested framework requires each item of data security regulation need to be done individually, for the operator's behavior pertaining every item followed and checked. The counting numbers system (agreeable numbers system) is dependent upon for following agreement levels of users for sometimes. Particularly, the grants points for acceptance behavior depend upon the agreement number's system idea, and reduction numbers for agreeable behavior. The data Technology Infrastructure Library (DTIL) is a framework enables effective and promotion of high technology activities in areas of computing. ITIL may provide check their threats, by putting processes in place for permitting and handle various incidences.

The implementation of data security within the institutions is achieved through this framework (Sheikhpour & Modiri 2012). COBIT 5 (Control goals for data and related computing assets) which is a highly recommended process or a model needed to perform various operations and processes of the institution's data security assets. Which give a model for assisting institutions to benefit in achieving goals and give additional output with high operations and running of the institution's data security computing assets (ISACA 2011).

**Table 4.7 Elements of data security policy**

| Security Policy | Security Policy Elements |
|---|---|
| Clean desk policy | Computer working areas should be secured when not in use is.<br>Anti-virus software should not be removed or disabled by employees.<br>Passwords, notes put or placed on or under computers by the employees require not to be left written down in an accessible location. |
| Password Policy | Every four months all passwords used like the one used for application, web, email and desktop accounts, all require to be changed. Adding to or writing of password in an email reports, carried using electronic methods exposed to a person through usage of the phone, or using questions or in security methods required shouldn't occur. |
| Internet Usage Policy | Downloading, visiting or viewing any illegal materials on the internet by employees should not occur. Employees should never download unauthorized software or files for use without getting permission from the IT department and their manager. |
| Email Usage Policy | Unprotected, sensitive or confidential information should not be sent by employees externally. Confidential institution's messages should not be forwarded to external locations . |

### 4.10.3 Checking Usage Behavior

Two methods have been used to record of data Security events (violations of the security policy) : from data security checking and protection tools (for instance where many users prolong social networks usage period or their passwords adjusting have not taken place for a long period) or is done manual from security written documents or managers who perform various processes (for instance where users computers are not locked ). The happenings occurrences may involve, but are not only to:

• Operation Managers: Users may perform data breaches with the data security regulations, for example a user giving out their password or their computer not locked up such behavior need to be reported.

• Internet usage: many institutions have fear of threats emerging from the internet exposes them greatly. Usage of social networks, downloads and cloud storage services by employees not taking into consideration the data security regulations that has been individually formed for the usage of the internet, this is a high big breach for the institutions, operator behavior pertaining the internet usage policy can be collected by a locally by the people concerned on network flow.

• Email usage: An operator's behavior pertaining the email usage policy can be collected by a local agent on an exchange server.

•Information application stage is a commonly used directory: of which all user accounts and passwords are kept track by such directory database. User behavior pertaining the password policy can be gathered by the person concerned with the active directory locally or at the level of applications. Every part of the policy type will be determined by monitoring users agreeability for the data security regulations.

The secret data of the users' the institution should be aware of it and protected at all times. So, the users need to be made aware of the checking process and it will not threaten their privacy in any way,

Meant for the certain behavior or behavior that does not comply, Such as, regulation for password for the user need not to be checked by itself; it's the attributes of passwords also creation date that need to be checked.

### 4.10.4 Overview of the Framework

To improve the allowed level of usage by the suggested framework it's depend upon the two major ways: taxonomy of the agreeable plan for the wrong behavior, and utilization of the agreed numbers system. Institutions may select the rights privileges for the wrong behavior that covers their needs. However, in the suggested framework the agreed method is pinpointed to involve two groups as a normal method:

Category 1: The data security regulation awareness improved

Category 2: Enforcing data security regulation

Non-agreed behavior may result in removal of points while an employee who agrees with the agreed points system, and portly good behavior will earn points,.

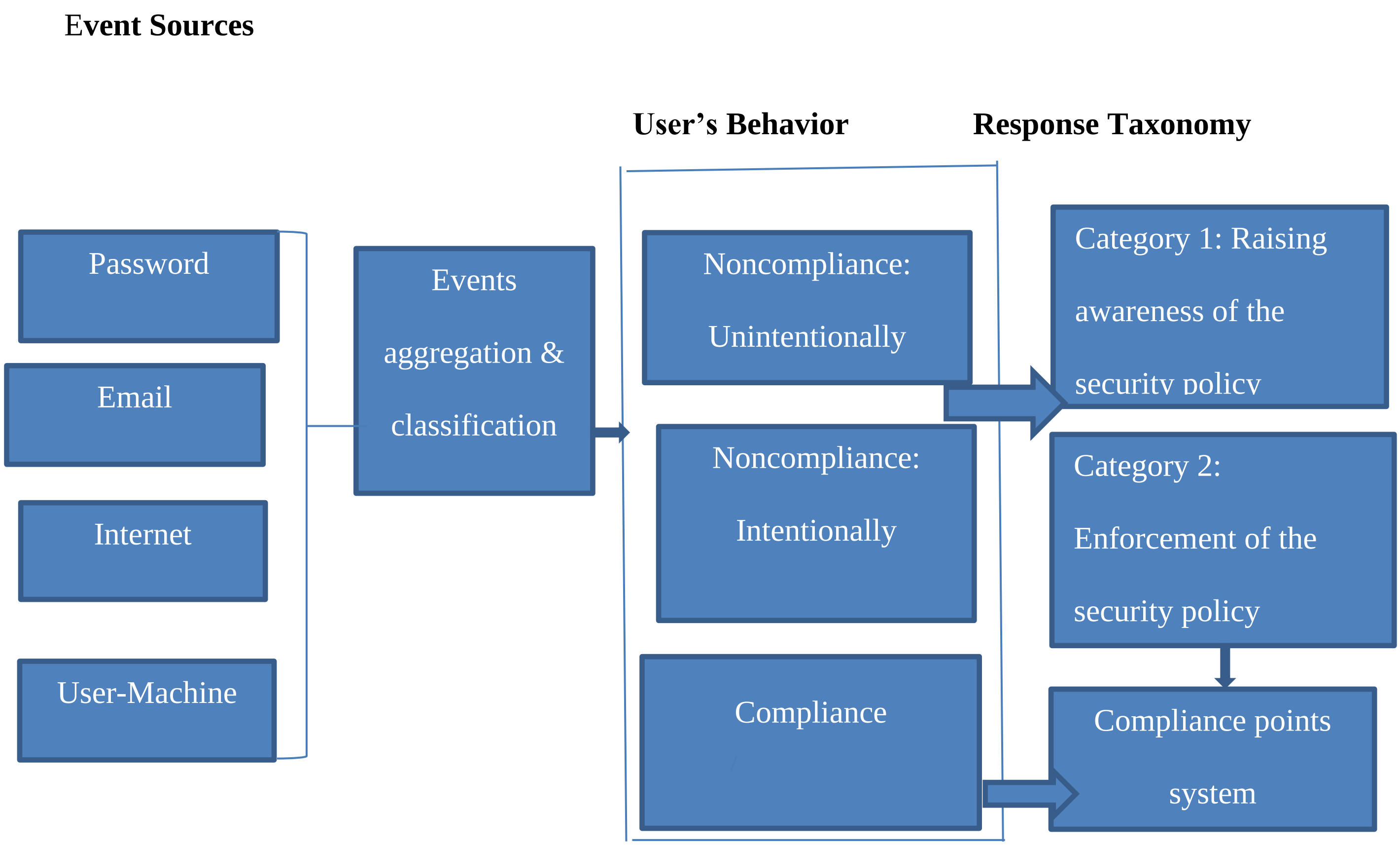

Event Sources
User's Behavior
Response Taxonomy
Password
Email
Internet
User-Machine
Events aggregation & classification
Noncompliance: Unintentionally
Noncompliance: Intentionally
Compliance
Category 1: Raising awareness of the security policy
Category 2: Enforcement of the security policy
Compliance points system

**Figure 4.9.1 Proposed Model Outline**

### 4.10.5 Users' Behavior

The behavior of the three proposed user pertaining the data security policies have been pinpointed: unintentional not-agreed, intentional not agreed and agreed. All these behaviors are determined all through the suggested framework.

1- Agreed behavior: The desired behavior of agreement is shown by the users through the security regulations.

2- Lack of awareness of the data security regulations is brought about by non-agreed behavior: user non-malicious behavior.

3- Non-agreed intentional behavior: the user violates with their full knowledge the data security policy, put in place all through non-compliance for the similar action for a specific period of time.

### 4.10.6 Non-Agreed Behavior for Response Taxonomy

The people of key concern for institutions are the employees that violate the data policies. High number of the institutions recently is using the old ways to improve and up data policies the users' awareness. (1) Data regulation for raising awareness, (2) security regulation enforcement of the suggested model has two methods of agreement for non-agreed behavior: Specific criteria consist of sub-responses that are made to improve severity levels gradually as shown below:

Category 1: The security policy of increasing awareness of (operation in two levels)

- Level 1: Data security regulations alertness given in written form and Yellow alertness (lowest level of improving awareness).

- Level 2: The online oriented exposure training, video oriented exposure alertness (High increase of exposure) and Orange alertness.

Category 2: The data security regulations enforcement (operation in two levels)

- Level 3: Reduction of IT privileges, limiting access or completely blocking access of direct intervention also affirming of data security regulations.

Any violation is increased from Level 1 to Level 3 due to the high level of response to, which the framework suggests of the three levels of response to non-agreed behavior.

But, institutions need to transform their perceptions towards the amount that fits for personal requirements.

### 4.10.7 System Compliance Points

The importance of agreeable points is mainly to boast the user's morale to be agreeable with their data security policy. Also it useful in indicating the current agreement level of every usage of every item of the data security regulations. The system agreeable numbers' depend mainly on two things: one, Earning points for the reward of good behavior, and their agreeable points' credit increases after each agreeable action a user agree with the data security policy. Also, the non-agreeable of data security regulations amount to decreasing numbers that could have gone higher or increased. Every item of the data security regulations has its own agreeable numbers' checker. Promoting required awareness, depending on checking the agreeable level for every element by the use of different checker on each element is important.  The agreeable point of every user pertaining the entire data security policy has an overall aggregated value. Notification should be given to the users needed for checking processes necessary for agreeable numbers also those that may come across such as of non-agreeable behavior. So, an institution needs to make ways to give all this data to all the users.

Within the proposed framework agreeable levels of usage which act as initiator for some activities or breaches. Such as, increased acquirement of agreeable numbers or increased level of agreeable number, an important way of any worker's following data security regulations. But, an incoming in reducing agreeable numbers which is a way of non-agreeable behavior, may be willingly or unwillingly. The rate or situation of agreeable numbers which start encouraging activities or awards for the specific behavior, which may involves:

- Gratitude letter or email for being a royal employee.
- Informing Human Resources (HR) to update an employee file.
- Awarding an employee with a mention on a board of excellence (Staff Excellence Award).
- Awarding a bonus or voucher for use in institutions facilities.

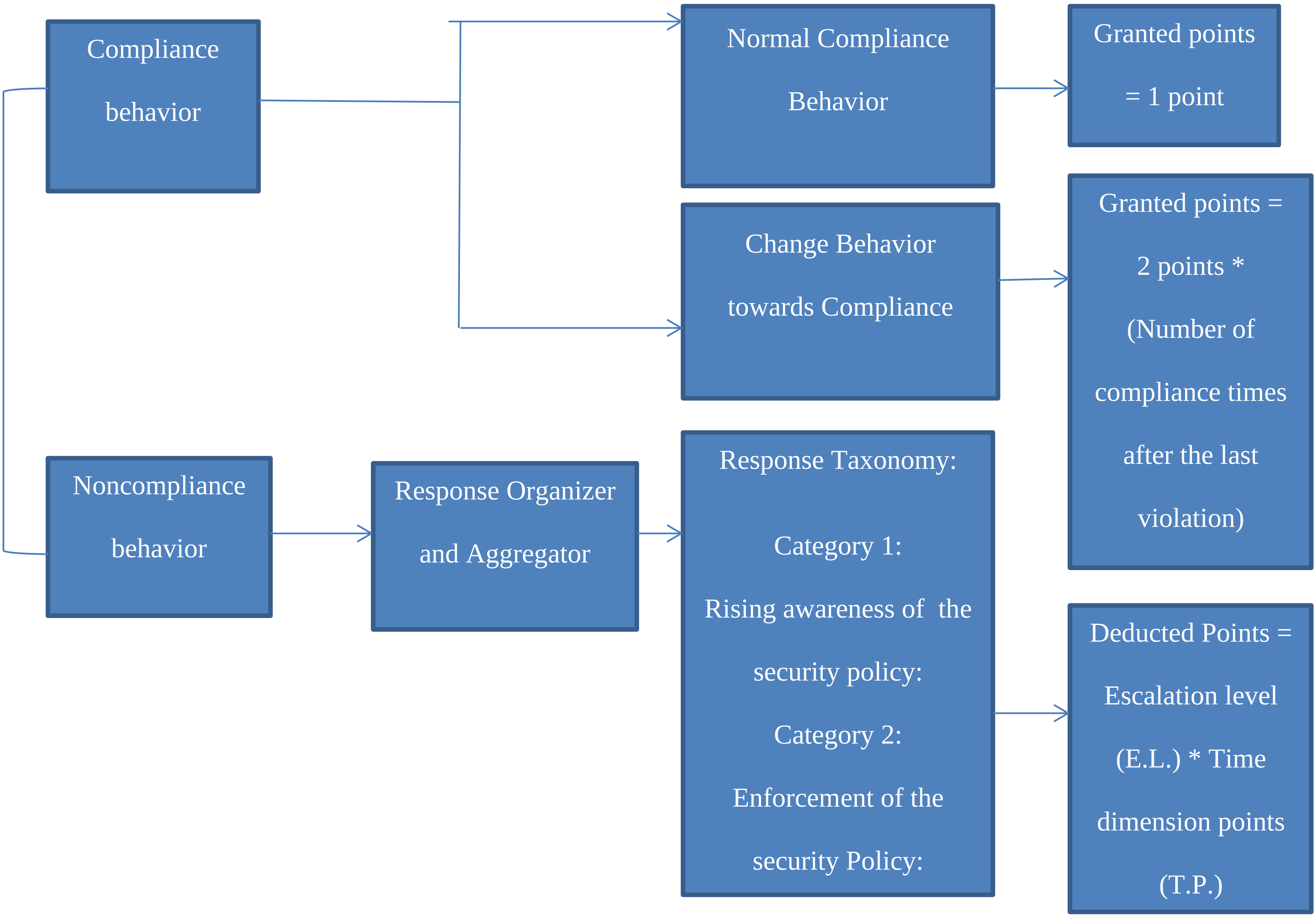

Compliance behavior
Normal Compliance Behavior
Granted points = 1 point
Change Behavior towards Compliance
Granted points = 2 points * (Number of compliance times after the last violation)
Noncompliance behavior
Response Organizer and Aggregator
Response Taxonomy:
Category 1:
Rising awareness of the security policy:
Category 2:
Enforcement of the security Policy:
Deducted Points = Escalation level (E.L.) * Time dimension points (T.P.)

**Figure4.9.2 A framework for monitoring end-user security policy compliance**

There are two different users behavior regarding the data security regulations: agreeable behavior and non-agreeable behavior. Suggested framework, included in Figure 4.9.2, its main purpose is meant for monitoring user behavior depending upon data security regulations. To monitor levels of the agreeability by users the agreeable numbers system is used. The following sections explain the framework in details.

### 4.10.8 Compliance Behavior

When a user portly the required behavior pertaining data security regulations and rules are considered to be agreeable to them. Two ways of checking users' behavior are required to count compliance.

1-The usage performances and various activities of royalty, for instance, changing of their password at an interval of six months in agreement to the regulations needing the target activities (transforming password regulations); depending upon on complete action, user are termed royal when they are not abusing data security regulations in given span or period, instantly, searching online by the user is not non-work or unrelated online work for a specific span for not less than two months depending upon a prolong given span ( agreed time).

2-users agreeing with data security regulations gain royal numbers due to behavior according to every item, and every item of the data security regulation has a different checker of numbers for every usage. Granting of points is done using two methods: points given for normal agreeable behavior and points given for transforming behavior towards agreeable (see Figure 4.9.3)

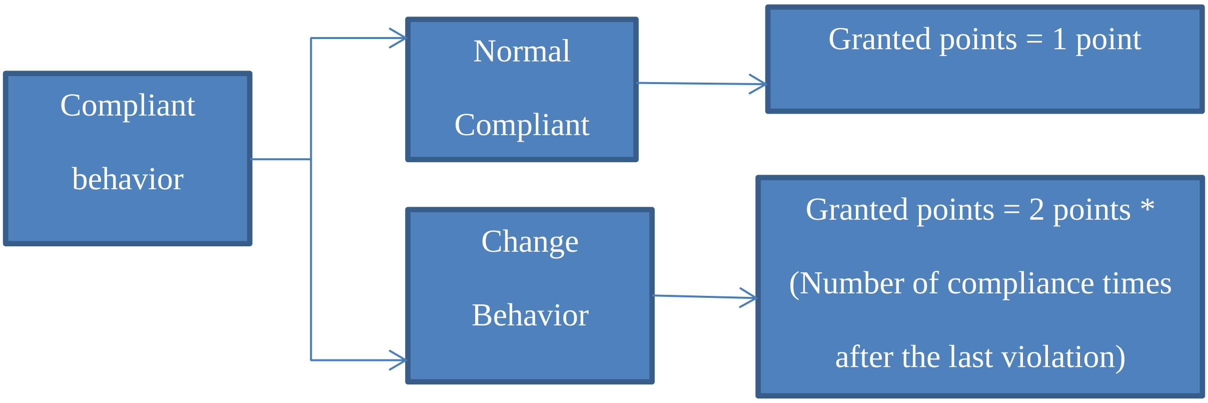

Compliant behavior
Normal Compliant
Change Behavior
Granted points = 1 point
Granted points = 2 points * (Number of compliance times after the last violation)

**Figure 4.9.3: Dealing with compliance behavior**

### 4.10.9 Normal Compliance Behavior

It is a good behavior that the users agree to the data security regulations a portion of their norm. The behavior is given 1 number rewarding every royalty every different data security regulations item (Point earned = 1 point).portlying, given category in Table 4.8. Portly that User A acted in agreed way in connection to two separate items of a data security regulations - transforming password data security regulations and not searching of online- download regulations.

**Table 4.8 Demonstrate Compliant Actions to Different Elements of a Security Policy**

| Action | Actions and Date | Policy Description |
|---|---|---|
| Action 1 | User A changed his password-01-01-2016 | Passwords must be changed every six months. |
| Action 2 | User A changed his password-01-06-2016 | |

| | | |
|---|---|---|
| Action 3 | User A did not browse non-work-related websites - 01-01-2016 to 01-03-2016 | Browsing non-work-related websites is prohibited. |
| Action4 | User A did not browse any non-work-related websites - 01-03-2016 to 01-06-2016 | |

According to Table 4.8, four points for User A data security agreed behavior pertaining the two items of the regulations. The first action earned 1 point when they changed their password in agreeable with the transforming password data security regulations, with total numbers.

Changing password by User A twice, totaling for the password changing regulation to 2 points for the regulation at 1 point this second action also getting another point. Figure 4.9.4: Granting points for agreeable behavior .The next behavior getting another point for three months due to User A agreeable, and because of this, all counts for lack of searching any online materials will be another point. Also, User A gets another point for being royal in finding of work not from online data security regulation, and due to this totaling specific data security regulation items to 2 points.

### 4.10.10 Agreeable Behavior Change

Number two methods, for all users transforming behavior for lack of royalty or agreement. This process main purpose for boasting the morale of users to continue agreeing with the data security regulation helping to continue getting additional counts, eventually gaining the points reduced due to lack of royal behavior. It helps returning the reduced points in a fast or slow way. The suggested formulae required for enhancing process is: Points transforming behavior = 2 points * (No. of agreeable behavior breach done lastly of the same regulation item).

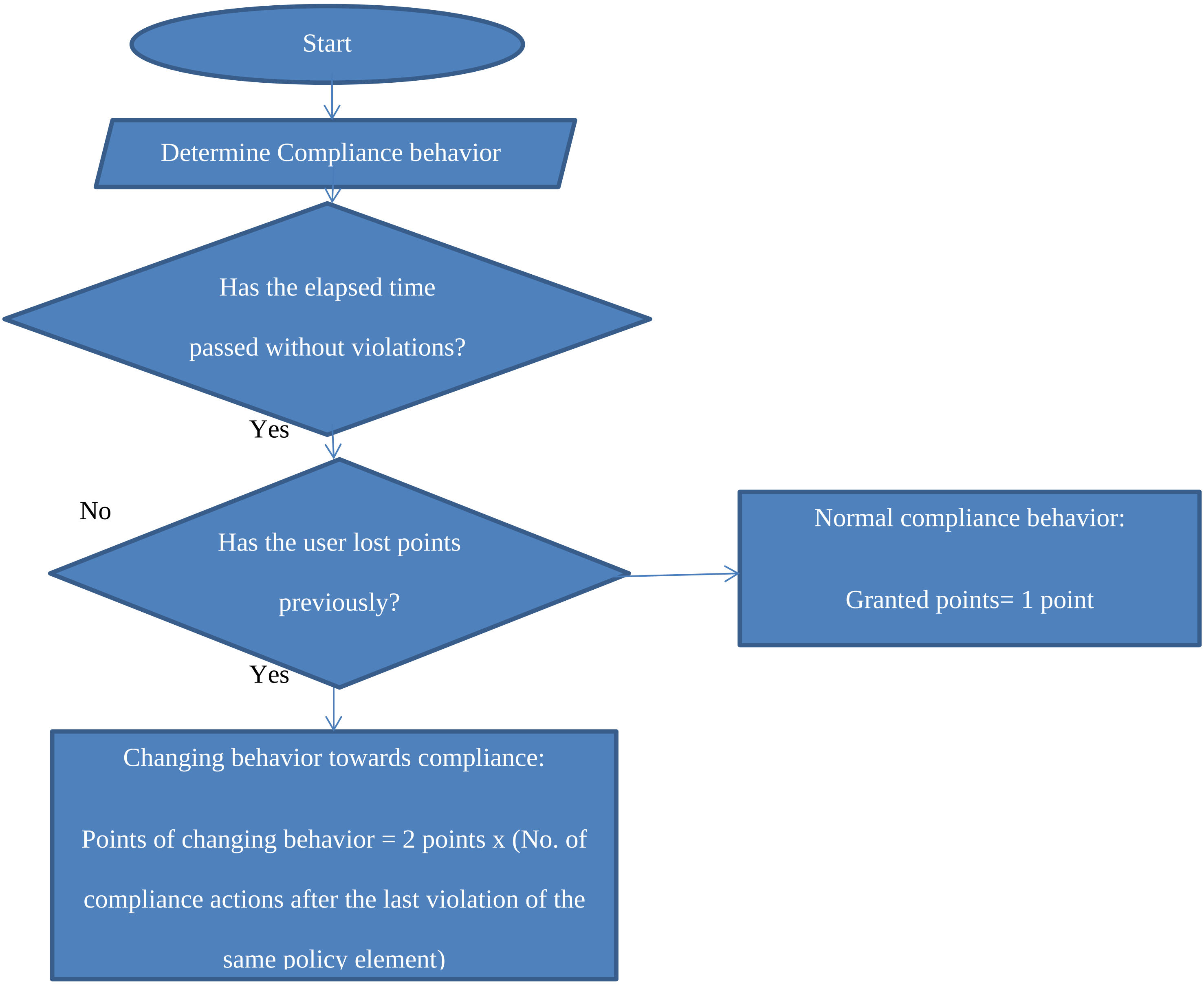

Start
Determine Compliance behavior
Has the elapsed time passed without violations?
Yes
No
Has the user lost points previously?
Normal compliance behavior:
Granted points= 1 point
Yes
Changing behavior towards compliance:
Points of changing behavior = 2 points x (No. of compliance actions after the last violation of the same policy element)

**Figure 4.9.4 Granting points for compliance Behaviour**

The Table 4.9 demonstrates User B not transforming password for more than 24 months, and this regulation needs every six months to transform. User B result in reducing points four times (24/6 = 4) due to breaching behavior. Transforming their password regulation they transform their behavior every time they comply with the policy User B earns more points which help in gaining the reduced points for that item. These three activities are shown in the table below.

**Table 4.9 Behavior Change Example for Compliance: User B**

| Action | Action and Date | Points Earned |
|---|---|---|
| Action 1 | User B changed his password 01-01-2016 | Points earned = 2 x (No. of compliance actions after last violation) Points earned = 2 x 1 = 2 points |
| Action2 | User B changed his password 01-06-2016 | Points earned = 2 x 2 = 4 points |
| Action3 | User B changed his password 01-12-2016 | Points earned=2 x 3 = 6 points |

In Activity 1, User B gained 2 points for being in agreement with this item of the data regulation, and due to this activity initially agreed after the final breaching. In Action 2, the points gained by User B have increasing to 4 points for it was the number two agreed, so the total points for this data regulation item are now 6 points. In Action 3, the third royalty of the user having a different password gained 6 points, the full amount for the regulation totaling to 12 points.

User B slowly increase points through transforming behavior of the user's royalty, but, this method stop when the user gains reduced points and changed back to the normal agreed process. More points could be provided for specific behavior to improve a specific behavior due to its importance or difficulty in an institution, Table 4.10. Demonstrate the other procedures for giving counts for agreed behavior.

**Table 4.10 Compliance points for compliance**

| Behavior | Points Earned |
|---|---|
| Normal compliant behavior. | 1 point earned for each instance of compliance |
| Changing and maintaining behavior towards compliance. | 2 points x (No.of compliance actions after last violation) will be earned by the user each time until they recover any lost points. The extra points are a reward for positively changing behavior. |
| Agreed to item with higher difficult or importance. | More points earned as a reward for part. |

### 4.10.11 Non-Agreeable Behavior

Non-agreeable behavior usage is monitored on transparent activities geared to the abuse of the data security regulation, such as getting unauthorized asset.

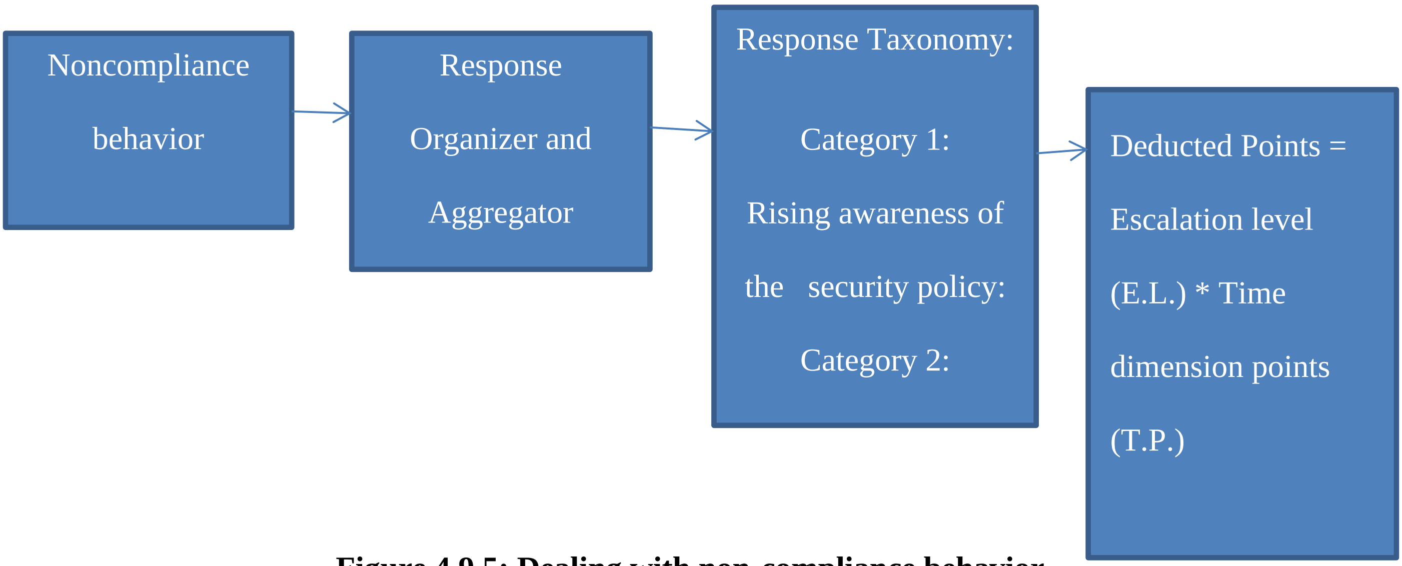

Noncompliance behavior
Response Organizer and Aggregator
Response Taxonomy:
Category 1:
Rising awareness of the security policy:
Category 2:
Deducted Points = Escalation level (E.L.) * Time dimension points (T.P.)

**Figure 4.9.5: Dealing with non-compliance behavior**

### 4.10.12 Aggregator and Response Organizer

The purpose of this part required for plan the procedures of adhering to for wrong behavior. Adherence requirement depends upon this part, for reduction of all points count.

The method of agreement depends upon addition idea for usage. Such as, responding to user’s manager email, also adding other abuse from other users considering the abuser’s behavior.

### 4.10.13 Response Taxonomy

To improve alertness or enforce the regulation data security of non-compliance behavior action plan is required. Hence, the non-agreeable behavior is proposed by two groups of agreement of the framework: (1) data security regulation for awareness improvement.

(2)Data security regulation affirmation. Moreover, every group is consisted sub- actions of various kind, meant for the severity levels very slowly and sure improvement.

Group 1: Data security regulation awareness improvement (improvement two stages)

Level 1: Writing of data security regulation updating &yellow alertness (Low alertness increase)

Level 2: Online-based alertness training procedure or online-video alertness update (High improvement alertness).

Category 2: Enforcing data security regulation (three stages occurrences)

Level 3: Enforcement the security policy and direct operation or e.g. preventing acquire some IT assets or decreasing rights of acquiring assets.

Agreement performance is increased by time given used as a sign of improvement up to the incoming stage. Time method is time period between abuses of the similar data security policy element. That is, given time span of the wrong behavior has occurred from the final misuse depending upon a certain item of the regulation. The following include three types of time method:

(1) Short period of time.

(2) Moderate period of time

(3) Long period of time

(Short time, moderate time and long time)of three types of time methods required to be changed by the institution , but the defaults values of the three types suggested by author as given out.

1- Short time dimension = default value of not than 24 hours. Due to, low time period for an important performance, making the time short.

2- Moderate time dimension = default value from 24 hours up to 6 months. Due to, adequate time from the final abuse and the user require to get an action from the final abuse.

3- Long time dimension = long span of time due to the user considered as a forgotten user the period between the current abuse and the final abuse should be i.e. a default value more than 6 months.

To show span period part on action plan for wrong behavior, Table 4.9.6 shows demonstrated case. User C abused given data security regulation, regulation 1, for more than a two-year severally for a period of time. The action plan for these abuses that have been assigned the following time values of the time used methods.

1-short time method = not than 24 hours

2- Moderate time method = 24 hours through 6 months

3-Long-time method = 6 months and above

**Table 4.11 User C violations**

| **Violation No.** | **Description** | **Date** |
|---|---|---|
| Violation 1 | User C violated policy 1 for the first time | 01-01-2015 |
| Violation 2 | User C violated policy 1 for the second time | 03-01-2015 |
| Violation 3 | User C violated policy 1 for the third time | 04-02-2015 |

| | | |
|---|---|---|
| Violation 4 | User C violated policy 1 for the fourth time | 09-05-2015 |
| Violation 5 | User C violated policy 1 for the fifth time | 10-05-2015 |
| Violation 6 | User C violated policy 1 for the sixth time | 12-01-2016 |

This policy has been abused by the User C six times over two years. On 01-01-2015 the first violation occurred, and the action stage was put to stage 1, low increased alertness. as such, it was the first abuse, there is no time method for current abuse and the previous abuse; hence due to c action stage is termed as stage 1. The abuse happened on 03-01-2015 for a second time, after the first four days, hence the time span considered moderate. For the second time user C abused the data security regulation willingly; highly improved alertness hence the action increased from stage1 to stage 2.

Almost a month from the second abuse the third abuse happened on 04-02-2015. The action increased to stage 3.The time dimension was considered moderate time span: Enforcement of regulation data security and direct intervention through preventing access completely lowering IT rights and decreasing access. The time span was considered as short time method when fourth abuse occurred at the same time as the third one. Action severity stopped at stage 3 hence no increment of action because both abuses happened in a short period span.

Two months after the fourth abuse another abuse occurred on 09-05-2015, and was considered as moderate time span. On 10-05-2016, exactly a year after the earlier abuse the sixth abuse happened, this is considered as prolonged-time span. The required action is only Level 1, lowest improved alertness due to this, there is no action increased to the next level.

As explained in this case with User C, the increased action of wrong behavior depends upon the time span type. The increased procedure depended upon on the time span type, the action plan is included of three stages, in which. The action plan for the next step is to fix the agreeable counts system.

### 4.10.14 Behavior for Non-Compliance Compliance Points System

Any non-agreeable behavior, with various processes used every time the stage of action abuse is increased over the behavior the points for the user are from their agreeable rate. Every improvement of action addition for the same abuses the count of points reduced down slowly for. The two factors determine the number of reduction points:

1) Improvement stage.

2) Time methods numbers

The time period type, short time, moderate time or long time, determined the improvement procedure of action from one stage to another and is used in the points' lowering formulae. Short time = 1, moderate time = 2 and longtime = 1. Each kind of time span has one point increment: Continually abusing similar regulation data security item while neglecting any action stage of improvement. Improvement stage of usage and the time method kind determines the number of counts of the framework decrement. The following is a formula of suggested method:

Decreased Points = improved level (I.l.) * time method points (T.p.).

The E.L. value is used together with the time method points, the improvement level the user already has. The time span determines the second point in the formula. Short period of time, moderate period of time and long span of time, and every kind is given a certain point producing three kinds of time span, which are: Short period of time =1, moderate period of time = 2 and long period of time =1.To differentiate the idea of the system agreeable points together with the action plan to wrong behavior, Usage by C's abuses is also looked at. The assumption is that Usage of C always neglected the improvement stages, in action to their wrong behavior with the regulation of data. Also, the agreeable points of C usage for this certain regulation of data are reduced for every abuse.

Abuse 1: On 01-01-2015 for the first time User C abused data regulation 1, hence E.L. Level 1 is determined by the time period category as long it is the first violation and: Reduction Points = E.L. x T.P. Reduction Points = 1 x 1 = 1 point, with -1 total for data policy 1.

Violation 2: On 05-01-2015 User C violated the regulation 1 for another time, the E.L. will be Level 2 and the time span is moderate span. (Moderate period points T.P. =2). So, Reduction Points = E.L. x T.P. Reduction Points = 2 x 2 = 4 points, with -5 points total for regulation 1.

Violation 3: On 09-02-2015 User C abused the regulation for the thirdly, the E.L. will be Level 3 and the time span is moderate span. (Moderate period points T.P. =2). So, Reduction Points = E.L. x T.P. Reduction Points = 2 x 3 = 6 points, with -11 points total for data regulation 1.

Abuse 4: User C abused the data regulation 1 on 10-02-2015 User C abused the data regulation fourthly, similarly the second abuse, the time duration is short for E.L. Level 3. B

The abuse happened or followed the earlier one, there was no improvement in the next level. Reduction Points = E.L. x T.P.     Reduction Points = 3 x 1 = 3 points, with -14 points total for regulation 1.

Violation 5 On 10-05-2015 User C abused the data regulation fifthly, the time span is moderate and the E.L. will be Level 3. Reduction points = E.l. x T.p. reduction points = 4 x 2 = 8 points, with -22 points total for data regulation 1.

Violation 6:   On 12-05-2016 User C abused the data regulation sixthly, one year after the earlier abuse, the E.L. will stop at stage 4 and the time span prolong. (Long span points = 1).

Reduction Points = E.L. x T.P. Reduction Points = 4 x 1 = 4 points, with -26 points total for data regulation 1, since this abuse happened a long time after the earlier one.

#### 4.10.15 Importance of the Suggested Implementation Model

Ideas mainly necessary are two: taxonomy of the action plan to wrong behavior, and using point's system agreement. The action taxonomy of wrong behavior includes two groups: increasing awareness and affirming the regulation data security. Points for agreed behavior are used to give the agreed points system, and reduce points from non-agreeable behavior. This type has been built to meet institutions' needs for increasing users' compliance with data security policies. Conformity with regulation of data security needs increment through giving users with a dynamic response to their behavior.

The individualized and personalized of increasing awareness is main purpose of the suggested framework. When non-compliance behavior has happened, there are aimed responses for every employee. Every usage is needs a specific action, required to increase security alertness, depending upon right behavior happenings action category aimed on the item of the data regulation frequently abused. Regulation item having low complying stages: huge number of user abuses of item of the security regulation requires quick research pertaining this item of the regulation to boast its performance.

Effective data security awareness programmes is achieved by technology accepted to propagate regulations as indicated by Qudaih et al. (2014).

An institution can frequently update and review its policy pertaining every data item security regulation by checking user's behavior.

It's an indication that all input given to improve complying with the item has gained in benefiting from aims of each item has a high stage of usage complying of the security regulation.

Users' action behavior built agreed points system, either giving points as award or reduction points for not complying. Every item of the regulation total points from all users make the measurement process of complying. Consequently, the extent of users' complying is measured using the level of complying points of each item of the regulation. All user abuses of any item of the security regulation are monitored using suggested framework. Information for any user abuses can be important for an institution, such as in data investigation or breach checking User's level of agreed points for every item of the regulation:

For every item for data security regulation usage multiple complying points, where the points go up with agreed behavior or go down with user abuses. Hence, it will be clear for an institution to monitor user behavior with every item of the security regulation by checking at the usage's stage of agreed numbers.

Institutions require comply with security regulation, also parts and operations of the framework are accommodated through designing this framework. A new method can be generated on complying with security regulations improvement through giving users with a dynamic response to their behavior.

# CHAPTER FIVE

## 5.0 SUMMARY, CONCLUSION AND RECOMMENDATIONS

### 5.1 Introduction

In this chapter, the findings are summarized, conclusion drawn and recommendations made in line with the study research objectives. The purpose of this study was aimed to find out the factors for effective information security control systems in public and private colleges in Nairobi County.

### 5.2 Summary of Major Findings

Effective information security control systems in public and private colleges in Nairobi County was influenced by four factors; Security awareness, information security control methods, security policies and information systems environment practices this led to effective adaption and integration of security control systems in public and private colleges Nairobi County**(N**=153**)**.

### 5.2.1 Security Policies in Public and Private Colleges in Nairobi County

The study findings from ICT Security experts confirmed that full adoption of recommended practices and guidelines were not receiving necessary approval and recognition of all levels of workers in the organization, 33.3% of respondents agreed and indicated that they have a positive impact in achieving effective Information systems security control which enhanced systems reliability in colleges in Nairobi County. 39.2% of respondent indicated that they have not complied with college security systems control policies in achieving effective Information systems security control, but only 5.9% who have appropriate college security control policies in private and public colleges in Nairobi County.

The study findings from 39.2% of ICT security experts respondents confirmed that, there were no security policies control procedure implemented so that the users may have well advanced data protective methods recommended to ensure all the workers of within the institution, other stakeholders and outside users, require to have adequate training and education, hence this affected implementation of government security control policies, 51% of respondents disagreed with no extent responses that there no government security control policies implemented and properly adopted in their respective colleges.

### 5.2.2 Security Awareness in Public and Private Colleges in Nairobi County

The study findings from47% respondents of ICT Security experts confirmed that no employee orientation and end users security control systems training for information technology security, only 19.6% of respondents who had security control systems user's support personnel in their college. The study revealed various data threats and breaches may be facing the institution private data, due to insufficient knowhow, skills and wrong altitude towards the proper and effective data protection by the workers, which contribute to big losses in the institution, due to lack of security control systems confidentiality agreement which was not fully used and utilized in colleges as indicated by 54.9% of respondents whom strongly disagreed.

The study findings from37.3% respondents disagreed that there was no security control disciplinary procedures put in place, a legal disciplinary process for workers involved in data breaches or done a data crime was required, only 21.6% indicated that they have contributed in achieving effectiveness of data protection control systems control in private and public colleges in Nairobi County.

### 5.2.3 Security Access Control Methods in Public and Private Colleges in Nairobi County

The study findings from 58.8% of ICT security expert's respondents confirmed that Enforcing compliance in security policy duties, areas of responsibility segregated and having procedure for Access Rights Review variables indicated that they have a positive impact in achieving effectiveness of the Information systems security control but only 19.6% have integrated and adapted security control systems access right reviews management in public and private colleges in Nairobi County.

The data protection patterns mostly concerned with the improving ways and methods of facilitating common needs, adapting user' registration procedure plan for security control systems with alignment of private data protection and all institute processes and enables the recommended data protection framework to align with the management, workers and other stakeholders outside the institution using data protection control systems, which may result to effective data protection.

Therefore, 56.9% of respondents strongly disagreed that there had adapted user' registration procedure plan for security controls in learning institutions that were needed for information security registration amongst the employees so that to enhance information systems effectiveness within the institutions.

### 5.2.4 Information Systems Environment Practices in Public and Private Colleges in Nairobi County

Various colleges respondents on information systems environment practices on whether they had adapted recommended ISO standards for effective diffusion of security control systems.

Which included ISO 9001:2015,ISO 9001:2008 ITIL, COBIT and NIST 800 series, 49.0% of respondents strongly disagreed that their colleges had adopted recommended standards.

These standards are promoting effective data protection and privacy through proper auditing, monitoring, validation and evaluation of data protective devices and control systems within private and public technical.

27.5% of respondents strongly disagreed that monitoring of security control systems was improving reliability of services delivery, but only 35.5% of respondent agreed that monitoring of security control systems will improve reliability of services delivery in public and private colleges in Nairobi County. The Information Systems Audit and Control Association (ISACA), and the IT Governance Institute (ITGI) in 1992 came up with Control Objectives for Information and related Technology recommended for the adoption as good guidelines and framework for IT operation within the institutions. Information Systems Audit and Control Association highly recommended COBIT for maintaining proper data protection standards internationally in the institutions to protect data against data threats and breaches.

Therefore 43.1% of respondents were in agreement that security control audit was enhancing quality of information in Technical Training Institutes in Nairobi County.

## 5.3 Conclusion

The objectives of the study were to determine the effects of security policies on information security control systems, impact of security awareness on information security control systems, to examine how information security control access methods affect information security control systems and to establish how Information system environment practices affect Information security systems in Technical Training Institutes in Nairobi County.

The study findings from ICT experts' professionals indicated that the information security control environment in Technical Training Institutes in Nairobi County is not ready to cope effectively with all information security risks. A majority of Technical Training Institutes in Nairobi County are not in a position to cope with information security threats. The conclusions were based on the objectives as follows: on objective one, the conclusion is that proper implementation of government and college security policies influenced the effectiveness of information security control systems. Security control systems in Education can serve as foundation of proper data protection and privacy as well as good data practices and guidelines as stated by (Peltier et al. 2005).Objective two, the conclusion was that workers of the organization, stakeholders and other users, to receive adequate awareness and influenced the effectiveness of information security control systems in Technical Training Institutes in Nairobi County.

Stephanou&Dagada, (2014) stated that in their investigation of information protection knowhow and education on information protection behavior was critical to any information security programme. Objective three, the conclusion was that information security access control methods influenced the effectiveness of information control systems.

Musa, (2014), indicated that permitting and allowing users the right level to access the data protection systems is highly recommended, for example delete and read access should be separately permitted to a specific person in need to access the data protective devices and data control systems. Denying the access the user after three invalid attempts, inactivating unused accounts and setting expiration dates on accounts are also good data protection methods. Objective four, the conclusion was that information systems environment practices influenced effectiveness of information control systems.

Research involving a survey of information security professionals from multiple industries (Steinbart et al. 2013) found out the improved on data protection ICT experts altitude about proper data protection and control in the private and public technical colleges in Nairobi County depended upon the correlation between the data protection and internal audit and validation.

### 5.4 Recommendations on Research Findings

This research recommends that the challenges and constraints hindering  affecting effective information security control systems in public and private technical colleges in Nairobi urban -urban region could be addressed through the following initiatives: The Ministry of Higher education must explore and recommend ways that ensure adaption of recommended ISO standards, security polices, information best practices and ensure there is access to the required technological tools, standard security software's and Network infrastructure.

#### 5.4.1 Security Policies in Public and Private Technical Training Institutes in Nairobi County

Proper protection of Security information systems should be done: Keeping data well protected and secured by permitting authorized users in the data protective devices and control systems.. Proper protection of information systems helps to protect information from being hacked.

Valuable information must be protected because is one of the most valuable assets of any enterprise. Prevention of unauthorized access to all information should be done: The prohibition and prevention of private data from hackers, malicious and ill motivated workers in the college institutions data protection systems.

### 5.4.2 Security Awareness in Public and Private Technical Training Institutes in Nairobi County

Appropriate awareness training of the organization workers and other outside users should be put in place; also they should receive regular updates in organizational practices and procedures as required for their specific jobs. All security issues and the need for security should be notified to all employees. Authorized users should be aware and trained in their responsibilities to help prevent unauthorized user access leading to an undesirable event. During recruitment Security functions should be well highlighted to all the employees. Before employment, organizations must make sure that all the workers and other outside users understand their roles, and are  good for the tasks they are entrusted for ,hence reducing the risk of theft, fraud or misuse of facilities. Employee's orientation for information and IT security should be done; also the employees must be reputable custodians and are required by law to protect the privacy of personal data belonging to the faculty, students and staff.

### 5.4.3 Security Access Control Methods in Public and Private Technical Training Institutes in Nairobi County

All information systems and services should be well secured for permitting and denying access to all data facilitated by putting appropriate user registration and de-registration policies in place. Secure log-on procedure should be put in place that would recognize a person authorized and permitted to access the data protection. Appropriate authenticating security method is required in selecting the permitted and authorized users. Systems with very sensitive information should have a specific (isolated) computing place. To ensure that the rights correspond with specific functions and responsibilities, various guidelines for Access Rights require constant evaluation by ICT data protection experts for that specific operation only.

Also all the system user requests need registration using guidelines stipulated in the activity carried out. The adoption of this guideline reduces non permitted users in private data and assets. To have and remove users from the data protection systems and processes the management require to have a good framework tail made to fit the needs of the private and public technical colleges.

### 5.4.4 Information Systems Environment Practices in Public and Private Technical Training Institutes in Nairobi County

Information security control systems require secure sockets layer (SSL) to ensure secure web transactions. This is a good protocol to protect the users during transfer their data by creating secret method separating private communications from the public Internet. It may facilitate Technical Training Institutes to have effective communications online free from data breaches and threats.

To ensure secure information systems, SSL (Secure Sockets Layer) should be put in place which provides an encrypted link between a web server and a browser. SSL is a recommended guideline which is used by all websites in the protection of their online transactions with their various users. The link provides all data passing between the web server and browsers remain private.

## 5.5 Recommendations for Further Research

The research focused on the data which is well protected from various data threats and breaches in data protection and control systems in public and private Technical Training Institutes in Nairobi County urban area. Further studies need to focus on challenges facing effective information security control systems in urban-rural and rural in public and private Technical Training Institutes.

## REFERENCES

Abu Musa, A.A. (2007). Evaluating the security controls of CAIS in developing countries: an examination of current research, *Information Management & Computer Security,* Vol.15 Issue: 1, pp.46-63.

Alahboul (2010): Impact of Information Security Policies on Computer Security

Arnason, S.T. &Willet, K.D. (2008).*How to Achieve27001Certification: An Example of Applied Compliance Management.* New York: Auerbach Publications.

Box,D.&Pottas,D.(2013).Improving information security behavior in the healthcare context", Procedia Technology, Vol. 9, No. 2013, pp1093 – 1103.

Bulgurcu, B., Cavusoglu, H. &Benbasat,I, I.(2010).Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness", MIS Q, Vol. 34, No. 3, pp523-48.

Bragg,B.(2011).CommonISO27001Gaps[online].Available:http://www.dionach.com/pdf/Common-ISO-27001-Gaps-ISSA0111.

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

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

Chaulaa, J.A., Yngströmb, L. &Kowalskic,S.(2017).*Framework for Evaluation of Information Systems Security.* Stockholm University/KTH, Sweden.

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

COBIT.(1998). *COBIT: Control Objectives*. ISACA, Rolling Meadows, IL. Corporate Commission of Higher Education (2012).*Status of Universities in Kenya* [online]. Available at: http://www.che.or.ke/status.html.

Cooper, R.B. and R.W. Zmud (1990) "Information Technology Implementation Research: A Technological Diffusion Approach," *Management Science* (36)2.
Cyberoam 2015 Cyberoam Technologies:www.Cyberoam.com

Davis, F.D. (1989) "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology", MIS Quarterly (13) 3.

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

Deloitte East Africa (2011).2011 East Africa Application Security Survey, safeguarding the future[onlineAvailable:http://www.deloitte.com/view/en_KE/ke/eamedia/kepublications/.sur vey reports/index.ht.

Education Center for Applied Research (2003).*Information Technology Security: Governance, Strategy and Practice in Higher Education* [online],Volume5.Available at:http://net.educause.edu/ir/library/pdf/ers0305/rs/ers0305w.pdf.

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

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

Government of Canada.(2012).*Audit of System Access Controls.* Internal Audit and Accountability Branch Citizenship and Immigration Canada Final Report May 2012

Government of Canada.(2017).*Audit of System Access Controls.* Internal Audit and Accountability Branch Citizenship and Immigration Canada Final Report.

Hau,D.(2017).*Unauthorized Access–Threats, Risk, and Control.* Global Information. Assurance Certification.SANS Institute.

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

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

Institute of Standards and Technology (2007).*Information Security Recommended Information security controls for federal information systems, Special Publication 800- 53,*

*Revision3*[online]http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.p.

International Journal of Management Excellence Volume 3 No.1 April 2014.Challenges Facing ISSM in higher learning institution.

Ismael (2011):Information Security Management Systems: Risk Management Course

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

ISO27k Forum (2011).*The Free ISO27k Toolkit: ISO/IEC 27001 Gap Analysis and Statement.OfApplicability*[online].Availableat:http://www.iso27001security.com/html.

Jeyaraj, A., Rittman, J.W.and Lacity, M. C. (2006) “A Review of the Predictors, Linkages, and Biases in IT Innovation Adoption Research”, Journal of Information Technolog(21)1,pp. 1–23.

Kashorda, M. (2007): *Emerging Trends in information and communication Technology Education in Kenyan Universities.* Strathmore University Press, Nairobi.

Kasomo, D. (2006). *Research methods in humanities and education.* Eldoret, Kenya: Zapf.

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

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

Laudon(2012).ManagementInformationSystems12th Edition:www.pearson.com/uk/educators/ higher-education...

Lee, S.M., Luthans,F.and Olson, D.L.(1982).A management science approach to contingency models of organizational structure, *Academy of Management Journal*, Vol. 25 No. 3.

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

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

Michael Nieles, Kelley Dempsey and Victoria Yan Pillitteri (2017) *Computer Security Division Information Technology Laboratory* U.S. Department of Commerce.

Ministry of Education (2007).*Press Release by Hon. Minister for Education - Friday, 25th May 2007 on the eve of "2nd International Conference on ICT for Development, Education and Training - E-Learning Africa*.

Musa, S. (2014).*Cyber security: Access Control.* The Evolution. Retrieved from https://evolllution.com/opinions/cybersecurity-access-control/ on 31/10/2017.

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

National Institute of Standards and Technology (2003).*Guide to Information Technology Security Services,* SpecialPublication80035.pdf.

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

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

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

National Institute of Standards and Technology (2007). *Guide to Secure Web Services, Special Publication 800-95*.pdf

National Institute of Standards and Technology (2002). *Risk Management guide for information Technology systems, Special Publication 800-30*.pdf.

National Institute of Standards and Technology (2007). *Guidelines for securing electronic messaging, Special Publication 800-.pdf*

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

Niles (2017):Common IT Security Risks in the workplace; www.ccsinet.com/blog/common-security-risks-workplace

Owens, R. G., & Steinhoff, C. R. (1976). *Administering change in schools*. Englewood Cliffs, NJ: Prentice-Hall.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M. &Jerram, C. (2014), Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q)", *Computers & Security,* Vol. 42, No. 2014, pp165-176.

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

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

Peltier, T.R., Peltier J., &Blackley J. (2005), *Information security fundamentals,* CRC Press.
Punch, K. (2008). *Introduction to social research: Quantitative and qualitative approaches.* SAGE Publication Ltd.

P.J., .Raschke, R., Gal, G., and Dilla, W. (2012). The relationship between internal audit and information security: An exploratory investigation. *International Journal of Accounting Information Systems* (13): 228-243.

Radack, S. (2011).*Continuous monitoring Of Information Security: An Essential Component Of Risk Management.* Information Technology Laboratory National Institute of Standards and Technology U.S. Department of Commerce

Reid, R.C. and Floyd, S.A. (2001).Extending the risk analysis model to include market insurance, *Computers & Security,* Vol. 20 No. 4, pp. 331-9.

RMAS.(2017).*InformationSystemsAudit.*HarvardUniversity.Retrievedfromhttps://rmas.fad.harvard.edu/pages/information-systems-audit on 2nd November 2017.

Robbins, S.P. (1994). *Management*, 4th ed., Prentice-Hall, Upper Saddle River, NJ. Steinbart,

Riley(2012):Rackspace Managed Security Minimizing Breach Windows: Rackspace Privacy and Data Protection: www.rackspace.com/data/protection.

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

Sante, T.S. and Ermers, J. (2009).*The IT Management Group TOGAF 9 and ITIL V3: Two white .paper*

Stewart, J. M., Tittel, E. and Chapple, M. (2008). *CISSP: Certified Information Systems Security Professional Study Guide, 4th Edition.* Indiana: Wiley Publishing, Inc 87 Tipton, Steinbart, P.J., Raschke, R., Gal, G., and Dilla, W. (2012).Information Security Professionals' Perceptions about the Relationship between the Information Security and Internal Audit Functions. *Journal of Information Systems* 27 (2).

Steinbart, P.J., Raschke, R., Gal, G., and Dilla, W. (2013).Information Security Professionals' Perceptions about the Relationship between the Information Security and Internal Audit Functions. *Journal of Information Systems* 27 (2).

Stephanou, A. &Dagada, S.R. (2008).*The Impact of Information Security Awareness Training on Information Security Behaviour: The Case for Further Research*. Conference Pape January 2008, South Africa.

Stephanou, A. &Dagada, S.R. (2014).*The Impact of Information Security Awareness Training on Information Security Behaviour.*

Stolarski, A.(2012).*Physical Access Control.* InfoSec Institute. Weber, R. (1999).*Information System Control and Audit*. Prentice-Hall, Englewood Cliffs, NJ.

Technology Group. (2008). *The threat within: is your company safe from itself?* Retrieved September 22, 2008, from Corporate Technology Group Web site: http://www.ctgyourit.com/newsletter.php

United States Department of Agriculture (2011). *FY2012 Information Security Awareness*

Wright, M. (1999).Third generation risk management practices, Computers & Security, Vol. 1999 No. 2, pp. 9-12

# APPENDICES

## Appendix 1.0 Research Questionnaires

### Information Security Experts Questionnaire

1. What is the category type of your college? Private college, ( ) Public College ( )

2. **Objective 1:** Rate your level of the agreement to what extent with the following statement by Tick where appropriate about the security policies affecting diffusion of information security control systems in your college.

| **Research Objective 1:**<br>What was security policies affecting effective Information security control systems in Technical Training Institutes in Nairobi County? To what extent your institution has achieved the following? | **Large Extent** | **Medium Extent** | **Undecided** | **Little Extent** | **No Extent** |
|---|---|---|---|---|---|
| To what extent your college has implemented government systems security control policies? | | | | | |
| To what extent your college has implemented higher learning systems security control policies? | | | | | |
| To what extent systems security control policies diffusion will enhance information systems reliability in college? | | | | | |

**Objective 2:** Rate your level of the agreement with the following statement by Tick where appropriate about the impacts on security awareness affecting information security control systems in your college.

| **Research Objective 2:**<br>What are impacts on security awareness affecting effective Information security control systems in Nairobi Technical Training Institutes? | **Strongly disagree** | **Disagree** | **Undecided** | **Agree** | **Strongly agree** |
|---|---|---|---|---|---|
| Do you agree that your college has trained end users on issues of information security control systems in teaching practices? | | | | | |
| Do you have security control systems orientation users' support personnel in your college? | | | | | |

| | | | | | |
|---|---|---|---|---|---|
| Do you think security control systems confidentiality agreement is fully used and utilized in your college? | | | | | |
| Do you have functioning disciplinary procedures in your college? | | | | | |

3. **Objective 3:** Rate your level of the agreement with the following statement by Tick where appropriate about information security access control methods affecting diffusion of security control systems in your college.

| **Research Objective3:**<br>How are information security access control methods affecting effective Information security control systems in Technical Training Institutes in Nairobi County? | **Strongly disagree** | **Disagree** | **Undecided** | **Agree** | **Strongly agree** |
|---|---|---|---|---|---|
| Do you think that your college has adopted user's registration procedures plan for security control systems as required? | | | | | |
| Do think your college has Integrated and adapted security control systems access right reviews management? | | | | | |
| Do you believe that institution management staff has segregation duties to manage security control systems in your college? | | | | | |

4(b. How many information security control systems do you have adopted in your college? Do you think the number of security control systems determines effective diffusion of security control systems? Elaborate your answer. ...........................................................................................

**.....................................................................................................................................**

5. **Objective 4:** Rate your level of the agreement with the following statement by Tick where appropriate about information security access control methods affecting effective security control systems in your college

| **Research Objective4**<br>What are Information system environment practices affecting effective Information security control systems in Technical Training Institutes in Nairobi County? | **Strongly disagree** | **Disagree** | **Undecided** | **Agree** | **Strongly agree** |
|---|---|---|---|---|---|
| Do you think your college has adopted recommended ISO standards for effective security control systems diffusion? | | | | | |
| Do you think monitoring of security control systems will improve reliability of services delivery in your college? | | | | | |
| Do you think security control audit will enhance quality of information in your college? | | | | | |

5(b. Do you have security control systems evaluation in teaching and learning in your college?

Explain.......................................................................................................................

.......................................................................................................................

## Appendix 2.0 LETTER OF INTRODUCTION TO RESPONDENT

Kisii University<br>
P.O. BOX 408-40200,<br>
NAIROBI.<br>
15th March, 2018.

Kisii University
P.O. BOX 408-40200,
NAIROBI.
15th March, 2018.

The principal,

Dear Sir/ Madam,

**RE: A FRAMEWORK FOR EFFECTIVE INFORMATION SECURITYCONTROL SYSTEMS IN TECHNICAL TRAINING INSTITUTESIN NAIROBI COUNTY.**

I am a student undertaking research in Master Degree of Information System in Computer System of Kisii University. My research is on the above topic. This research study investigated the policies affecting effectiveness of data protection and control systems in Technical Training Institutes in Nairobi County.

Kindly respond to the questionnaire given as correctly and honestly as possible. Be assured that your identity and response were to be accorded with utmost confidentiality. For this reason, do not write your name on the questionnaire. I look forward to your assistance and cooperation. Thank you.

Yours sincerely,

Rachael Wangui Kiroko

## Appendix 3.0: RECOGNIZED TECHNICAL TRAINING INSTITUTESIN NAIROBI COUNTY

Kenya Institute of Administration (KIA)

Kenya Institute of Management (KIM)

Kenya Institute of Mass Communication (KIMC)

Nairobi Institute of Business Studies (NIBS)

Kenya Utalii College (KUC)

Kenya Medical Training Centre (KMTC)

Kenya School of Monetary Studies (KSMS)

Kenya Technical Teachers College (KTTC)

Kabete Technical Training institute (KTTI)

Kenya Water Institute (KWI)

Railway Training Institute (RTI)

Pioneer's Training Institute (PTI)

Nairobi Technical Training Institute (NTTI)

Graffin's College (GCK)

Kenya Institute of Special Education (KISE)

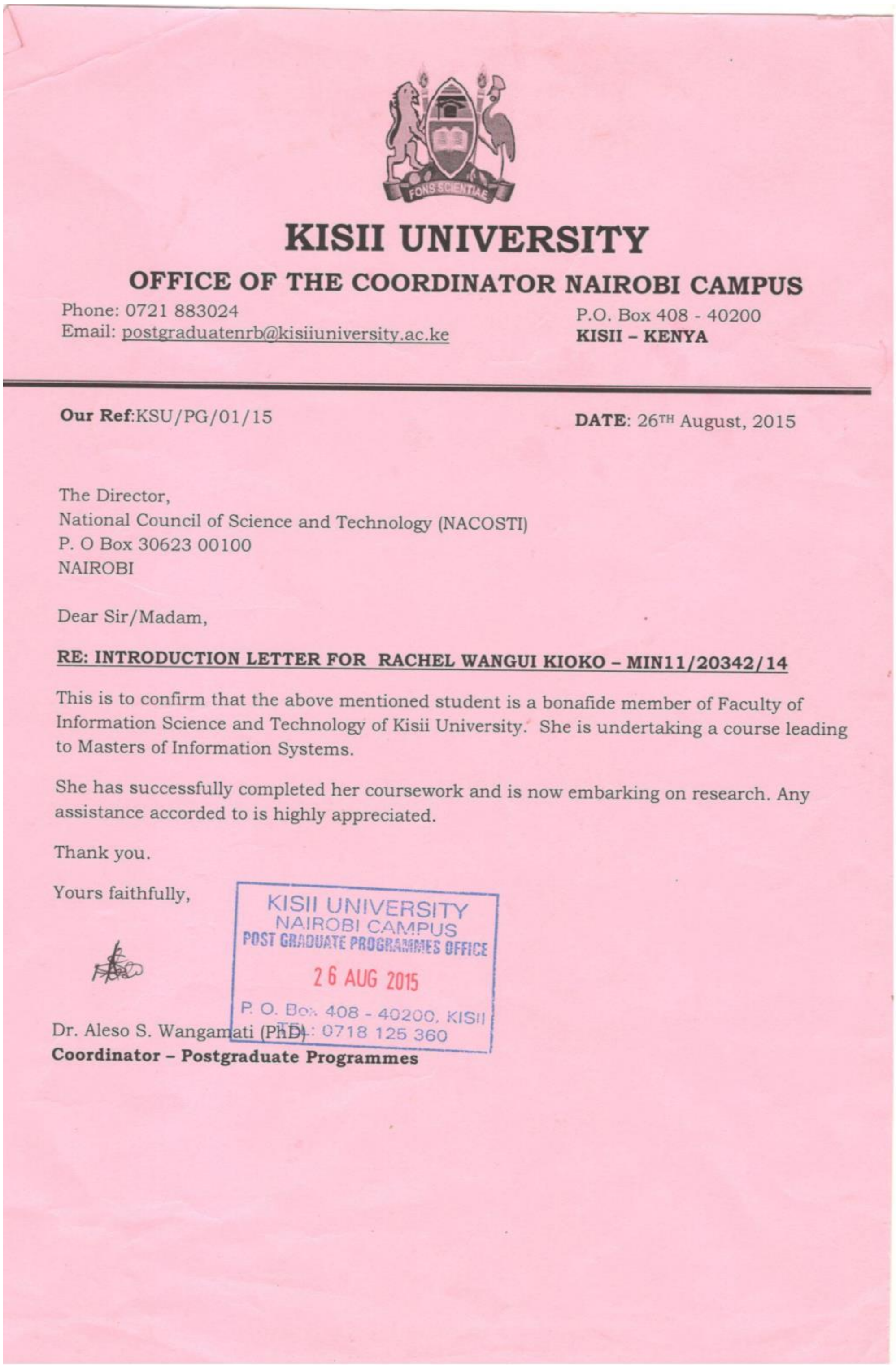
Kinyanjui Technical Training Institute (KTTI)

National Youth Service Engineering Institute (NYSEI)

Zetech Training Institute (ZTI)

Nairobi Institute of Business Studies (NIBS)

East Africa School of Aviation (EASA)



# KISII UNIVERSITY

## OFFICE OF THE COORDINATOR NAIROBI CAMPUS

Phone: 0721 883024
Email: postgraduatenrb@kisiiuniversity.ac.ke

P.O. Box 408 - 40200
**KISII – KENYA**

**Our Ref**:KSU/PG/01/15

**DATE**: 26TH August, 2015

The Director,
National Council of Science and Technology (NACOSTI)
P. O Box 30623 00100
NAIROBI

Dear Sir/Madam,

**RE: INTRODUCTION LETTER FOR RACHEL WANGUI KIOKO – MIN11/20342/14**

This is to confirm that the above mentioned student is a bonafide member of Faculty of Information Science and Technology of Kisii University. She is undertaking a course leading to Masters of Information Systems.

She has successfully completed her coursework and is now embarking on research. Any assistance accorded to is highly appreciated.

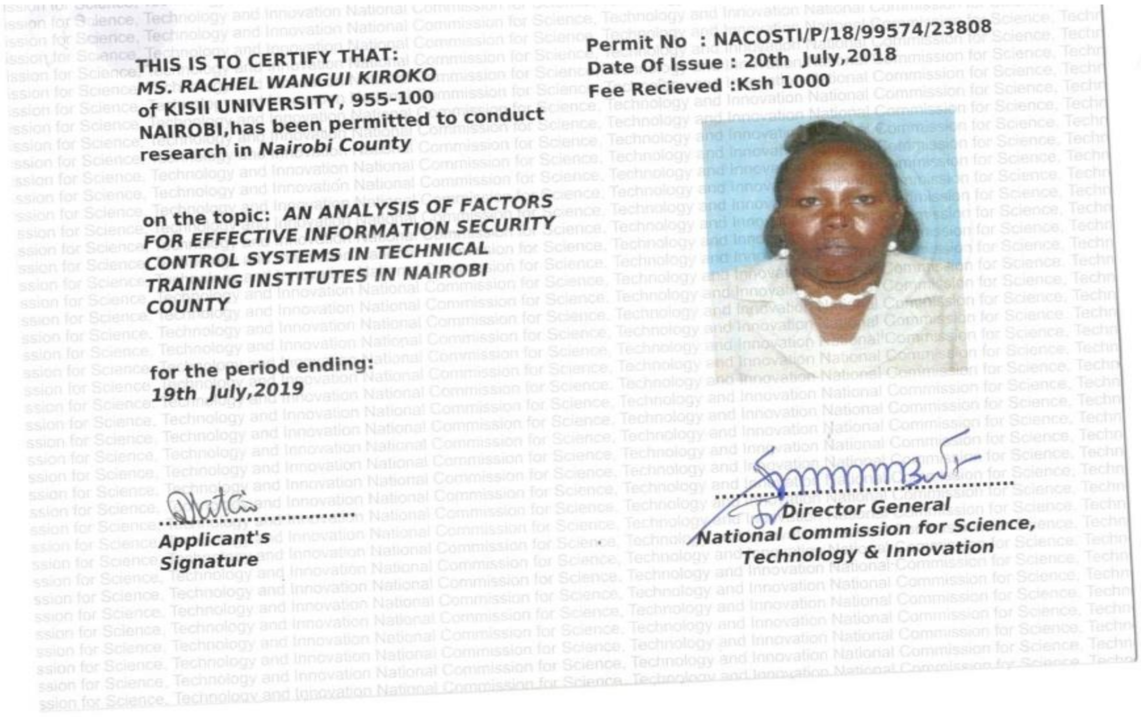
Thank you.

Yours faithfully,

KISII UNIVERSITY
NAIROBI CAMPUS
POST GRADUATE PROGRAMMES OFFICE
26 AUG 2015
P. O. Box 408 - 40200, KISII
TEL: 0718 125 360

Dr. Aleso S. Wangamati (PhD)
**Coordinator – Postgraduate Programmes**

**Appendix 4.0 Letter of Introduction from the University**



THIS IS TO CERTIFY THAT:
MS. *RACHEL WANGUI KIROKO*
of KISII UNIVERSITY, 955-100
NAIROBI,has been permitted to conduct
research in *Nairobi County*

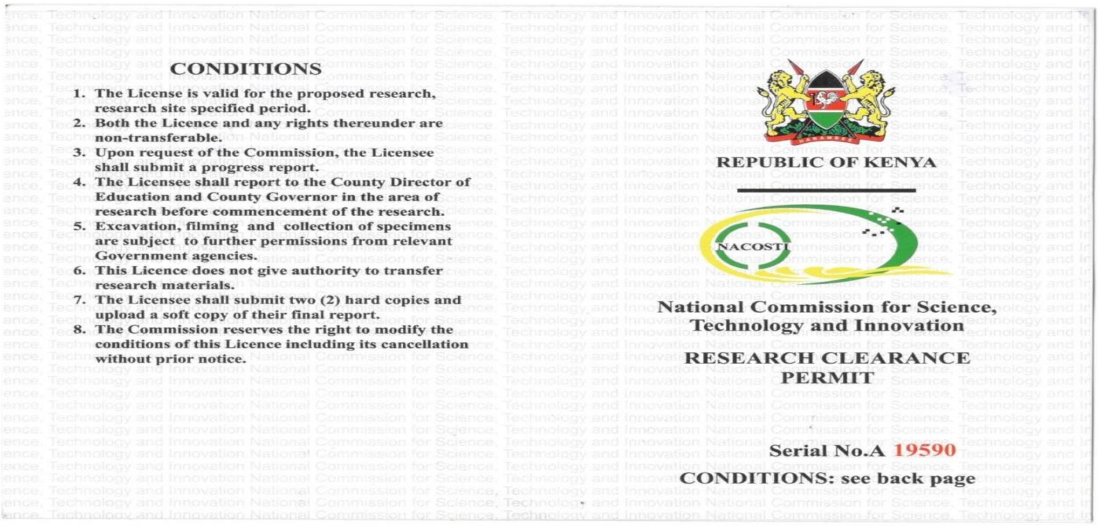
on the topic: *AN ANALYSIS OF FACTORS FOR EFFECTIVE INFORMATION SECURITY CONTROL SYSTEMS IN TECHNICAL TRAINING INSTITUTES IN NAIROBI COUNTY*

for the period ending:
*19th July,2019*

Permit No : NACOSTI/P/18/99574/23808
Date Of Issue : 20th July,2018
Fee Recieved :Ksh 1000

……………………
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

NACOSTI

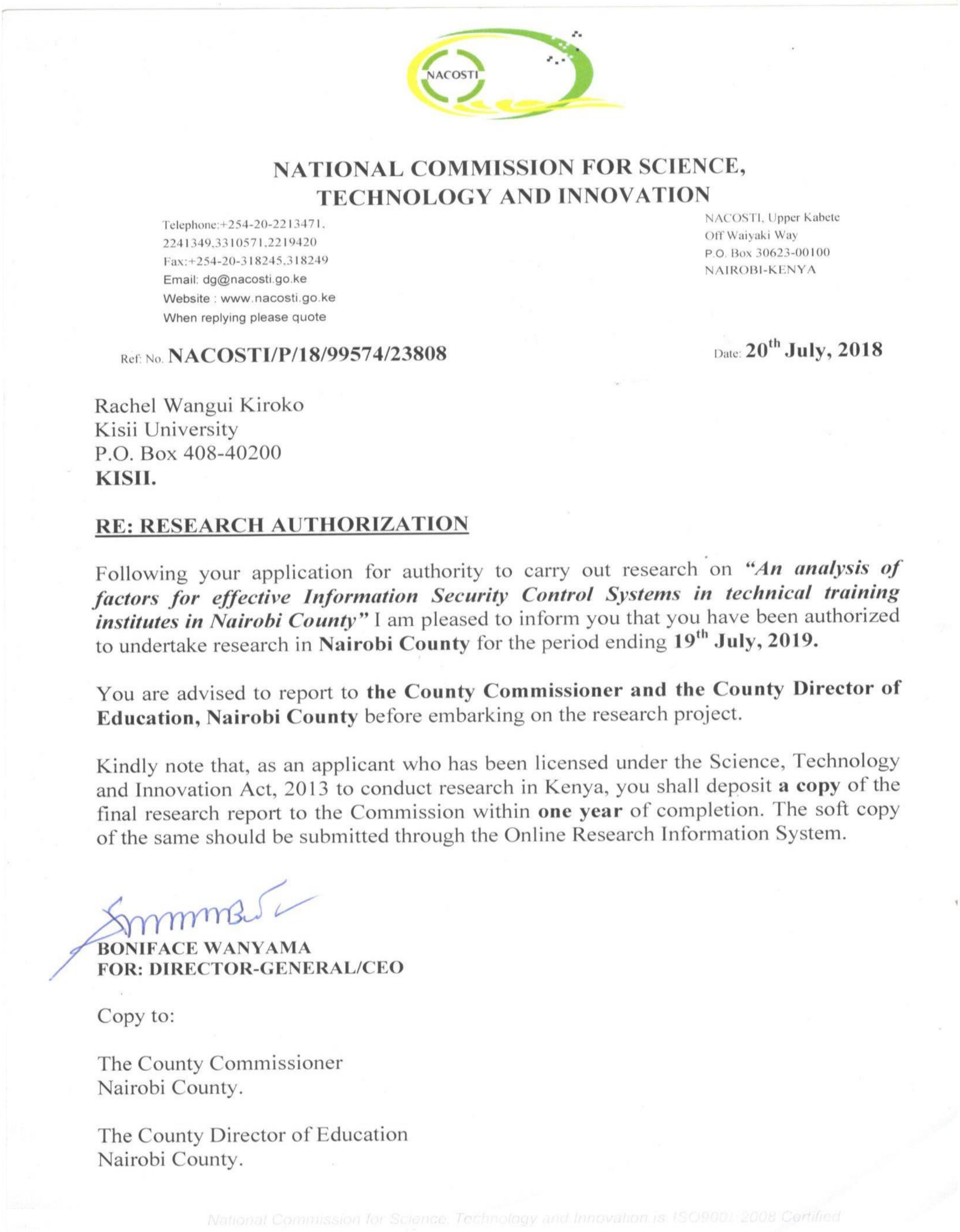
National Commission for Science,
Technology and Innovation

RESEARCH CLEARANCE
PERMIT

Serial No.A 19590

CONDITIONS: see back page

## Appendix 5.0 NACOSTI Research Clearance Permit



NATIONAL COMMISSION FOR SCIENCE,
TECHNOLOGY AND INNOVATION

Telephone:+254-20-2213471,
2241349,3310571,2219420
Fax:+254-20-318245,318249
Email: dg@nacosti.go.ke
Website : www.nacosti.go.ke
When replying please quote

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

Ref: No. **NACOSTI/P/18/99574/23808**

Date: **20th July, 2018**

Rachel Wangui Kiroko
Kisii University
P.O. Box 408-40200
**KISII.**

**RE: RESEARCH AUTHORIZATION**

Following your application for authority to carry out research on ***"An analysis of factors for effective Information Security Control Systems in technical training institutes in Nairobi County"*** I am pleased to inform you that you have been authorized to undertake research in **Nairobi County** for the period ending **19th July, 2019.**

You are advised to report to **the County Commissioner and the County Director of Education, Nairobi County** 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.

**BONIFACE WANYAMA**
**FOR: DIRECTOR-GENERAL/CEO**

Copy to:

The County Commissioner
Nairobi County.

The County Director of Education
Nairobi County.

**Appendix 6.0 NACOSTI Research Authorization**