# A WEB-BASED MODEL TO DETERMINE SECURITY RISK EXPOSURE INDEX AMONG SAVINGS AND CREDIT COOPERATIVE SOCIETIES

**MUTAI JOSHUA KIPROTICH**

**A Research Thesis submitted to the Institute of Postgraduate Studies and Research in Partial fulfillment for the award of Master of Science in IT Security & Audit of Kabarak University.**

**APRIL 2018**

# DECLARATION

I declare that this thesis is my original work and has not been presented for the award of degree to any other institution of higher learning

Signature ……………………………………… Date …… 14/05/2018….........................

**Joshua Kiprotich Mutai**

**GMI/NE/0738/05/16**

# RECOMMENDATION

This thesis entitled **"A web-based model to determine Security Risk Exposure Index among Savings and Credit Cooperative Societies"** was submitted for examination with our approval as University Supervisors.

Signature ………………………………………… Date ……May 15, 2018…........................

**Prof. Simon Maina Karume**

Department of Computing and Informatics,

Laikipia University

Kefa Rabah

Signature …………………………………………. Date ……May 15, 2018…........................

**Prof. Kefa Rabah**

Department of Computer Science and Bioinformatics,

Kabarak University

# COPYRIGHT

# DEDICATION

I dedicate this study to my beloved wife Gladys Mutai, sons Penuel Kiptoo Mutai and Perry Kibet Mutai, and my parents, Mr & Mrs John and Grace Boror

# ACKNOWLEDGEMENTS

I acknowledge the efforts of the people who encouraged, supported, and guided me during the period I was undertaking this research. First, I sincerely appreciate the support and guidance of my supervisors; Prof. Simon Maina Karume, Prof. Kefa Rabah and Dr. Nickson M. Karie. Secondly, I thank the members of my family who encouraged me and understood my absence the entire period I was undertaking the master program and particularly the time I was doing this research.

**Above all else, I thank our Almighty God for providing wisdom, strength, and wellbeing.**

# ABSTRACT

Savings and Credit Cooperative Societies (SACCOs), like other financial institutions, own critical assets that must be protected against attackers even as the threat landscape continue to persist. This study provides a solution to SACCOs by determining security risk exposure index (SREI) based on ISO/ 27001 standards. The objectives of the study were to determine the critical security risks factors affecting Selected SACCOs based on ISO 27001 standards, to design a model for computing their security risk exposure index, to implement a prototype as a web based application for computing security risk exposure index, and to verify and validate the model. The study targeted 55 respondents from 11 deposit-taking SACCOs licensed by Sacco Societies Regulatory Authority (SASRA) to operate within Nakuru County. The response rate of 90.9% was registered and was considered sufficient for the study. The design model was based on six of ISO 27001's eleven cardinal security control factors that were considered most critical to the security of the SACCOs using reduction analysis of the responses. Relevant Weights for computing SREI were derived and a mathematical model was designed. The model was implemented as a web-based prototype through design science paradigm using PHP as server-side language, CSS3 and JQuery for frontend styling and response, and MYSQL as a database engine. The designed model is significant in the sense that it provides the SACCO management and regulating authorities with useful information about security levels of their organizations when compared with best practices. The model provided appropriate actions necessary to maintain risk exposure to minimum levels.

**Key Words:** *Human Resource security, Physical and Environmental security, system security, Exposure Index, compliance, access control*

# TABLE OF CONTENTS

# LIST OF FIGURES

# LIST OF TABLES

# LIST OF EQUATIONS

# ABBREVIATIONS

| | |
|---|---|
| **CSS3** | Cascading Style Sheets version 3 |
| **DTS** | Deposit-Taking SACCO |
| **ERP** | Enterprise Resource Planning |
| **GUI** | Graphical User Interface |
| **ICT** | Information and Communication Technology |
| **IEC** | International Electro technical Commission |
| **ISMS** | Information System Management System |
| **ISO** | International Standards Organization |
| **MD5** | Message Digest 5 |
| **PHP** | Hypertext Preprocessor |
| **PWC** | Price Waterhouse Coopers |
| **SACCO** | Savings and Credit Cooperative |
| **SASRA** | SACCO Societies Regulatory Authority |
| **SREI** | Security Risk Exposure Index |
| **SQL** | Structured Query Language |

## OPERATIONAL DEFINITIONS

**Exposure** A system problem or error in software that relate to the software design and configuration that acts as a springboard for hackers by permitting access to information, information systems or network. (CVE, 2017)

**Index** An indicator or measure of something (Investopedia, n.d)

**Investment** The act of placing money or effort into something to make a profit or achieve a result: (Cambridge essential English dictionary, 2011)

**Model** A representation that can be graphical, mathematical, physical or verbal that provides a simplified version of a phenomena, structure, system, concept, or relationship of things in the real world (Farlex, 2009).

**Security Controls** These are administrative or technical countermeasures or safeguards to shun, counter, or reduce loss or inaccessibility because of threats that act on vulnerabilities (Northcutt, 2009)

**Security threat** Anything that may occur or may not occur but if it occurs; it has the potential of causing harm to information and/or information system (Techopedia, 2016).

**Web-based application** A software application that can be used over the internet through a web-browser.

# CHAPTER ONE

# INTRODUCTION

## 1.1 Introduction

This Chapter presents the background and the purpose of the study. It presents the statement of the problem, the study objectives, and the research questions. This chapter also introduces the significance of the study, expected outcomes, justification, scope, limitations, and the scalability of the study.

## 1.2 Background of the Study

Savings and credit cooperatives are a subset of wider cooperative movement. The International Cooperative Alliance (ICA, 2005) coined the definition of a cooperative as an independent alliance of people who willingly unite to uplift their social, cultural, and economic desires through commonly owned and democratically controlled endeavor. SACCO Societies Regulatory Authority (SASRA) notes a set of seven core values that drive all cooperatives as follows; democratic member control, open and voluntary membership, economic participation of members through one-member-one-vote basis, independence and autonomy, education/training/information, and cooperation. These principles are the ones that set cooperatives apart and make them distinct from other corporate or unincorporated legal entities (SASRA, 2015a).

SACCOs are notably adopting Information Communication Technologies (ICTs) to assist in performing their back-end operations. Although Kenya was behind developed countries in adopting electronic banking, the technology is gaining ground in the SACCOs and microfinance industry as a means of gaining competitive advantage (Koduk, 2015). Before the introduction of electronic systems in deposit taking financial institutions in Kenya, banking operations were manual which led to slow transactional processes (Atavachi, 2013). Today, the historical manual systems are being replaced with automated ICT systems, which are more efficient in running back-end business processes. There has been tremendous development in SACCO's growth in Kenya due to the adoption of electronic banking services that enhance operational efficiency and delivery of service to their customers (Chahayo *et al*., 2013). Based on research findings, the adoption of e-banking services by deposit-taking microfinance institutions is increasing as many of them begin to embrace technology (Atavachi, 2013).

Even though the government of Kenya through SASRA made attempt to see secure SACCOs by formulating guidelines on risk management practices, SACCOs focus on compliance to a sole requirement for implementation of Management Information Systems (MIS) in their organizations and fail to focus on the robustness of those MIS. The guidelines require them to install robust ICT infrastructure, define roles for board of directors and top management regarding the implementation of ICT policies and procedures. It is also important to install physical security, onsite and offsite storage of information, development and implementation of disaster recovery plans, infrastructure access, control and accountability, data backup and recovery, and ICT strategy to ensure that sufficient financial resources and human resources are assigned to sustain a steady and secure ICT setting (SASRA, 2015b).

However, reports indicate that SACCOs tend to focus their investments on customer satisfaction and cost reduction, and therefore overlook investment necessary for cybercrime prevention. As a result, they expose themselves as popular target for cybercriminals (Kigen *et al.*, 2016). Furthermore, these new technologies continue to be exploited by malevolent users and unlike banks, SACCOs lack skilled security personnel and anti-fraud systems and therefore it is very necessary to have a way in which the success of the cybercriminals can be averted and have the Sacco industry safe from threats (Kigen *et al.*, 2015).

Further reports indicate that every business that is connected to the internet has the risk of falling victims to cyber-crime at some point in time because cyber criminals are expanding their ability of stealing money directly or turning stolen data into money (Nyawanga, 2015). Maina (2017) that banks have turned out to be the principal targets of cybercrime as people gradually take up the use of financial technology agrees to this view. Further, Guguyu (2016) reported that a successful cyber-attack saw $81 million stolen from the Central Bank of Bangladesh in 2016 and that the Central Bank of Kenya and other government facilities could be the aim of impending cyber-attack. Further reports indicate that financial services organizations are 45% more likely to be attacked than other organizations (PWC, 2014).

According to Weluchi et al. (2017), there are varied challenges that SACCOs have to wake up concerning cyber security, they include; inadequate technical skills in SACCOs, lack of awareness among the management and the employees, legislation, low prioritization by the leaders, poor technical design of systems, social engineering practices. Additional set of challenges affecting financial institutions are highlighted by Dunkelberger (2017) as; heavy presence of threats on the threat domain. The dynamic nature of the threats, high pressure exerted by high consumer expectations, lofty compliance regulations, the risk of increased number of agreements, which the organizations engage with third-party vendors, human errors and insider threats. Additionally, this problem attributes to emerging technologies. With all this and more challenges, it is prudent to use best practices to check how exposed these organizations are to threats as they carry out their daily operations.

## 1.3 Statement of the Problem

Recent studies indicate that Savings and Credit cooperative societies have adopted ICT in their operations to improve efficiency and service delivery. Reports indicate that SACCOs hold their assets in form of information of members' savings, members' loans, buildings, technology systems, and personnel. However, the risk of SACCOs losing their assets continues to increase as new challenges are introduced to the threat domain such as insider threats, human error, emerging technologies, and increased third-party agreements. Notably, these financial institutions focus their investment on customer satisfaction and mechanisms of reducing operating costs and disregard the security of their assets. This negligence makes them more vulnerable compared to their counterparts in the mainstream banking industry. If SACCOs do not keep up with cyber security best practices, there are high chances of attacks given the increasingly sophisticated cyber space. This study sought to develop a model that would help the SACCOs, and possibly other organizations, to measure their level of exposure to risks and recommend appropriate control as per ISO 27001 standards for information security.

## 1.4 The Purpose of the Study

The purpose of this study was to develop a model that would help in determining Security Risk Exposure Index (SREI) for Savings and credit cooperatives in Kenya.

## 1.5 Research Objectives

The study objectives are:

i. To determine the critical security risks factors affecting savings and Credit Cooperative societies in Kenya based on ISO 27001 standards.

ii. To design the model for computing security risk exposure index of savings and credit cooperative in Kenya.

iii. To implement a prototype as a web based application for computing security risk exposure index.

iv. To verify and validate the model

## 1.6 Research Questions

The research questions are:

i. What are the critical security risks factors affecting savings and Credit Cooperative societies in Kenya based ISO 27001 standard?

ii. How will the model for computing Security risk exposure index in savings and credit cooperative in Kenya be designed?

iii. How will the prototype of a web based application for computing security risk exposure index be implemented?

iv. Can the model compute the Security Risk Exposure Index?

## 1.7 Significance of the Study

The study is significant to the following stakeholders;

i. The research informs the management of Savings and Credit cooperatives on the level of exposure to risks in their businesses. Hence, management can use the findings to strategize on appropriate countermeasures for securing their businesses.

ii. The findings of this research offer insight guide to the policy makers such as Sacco Societies Regulatory Authority (SASRA) in formulating and enforcing policies that governs information security and hence will help to minimize the levels of exposure of Sacco's information and information systems.

iii. This study will also add to existing literate on SACCOs and information security risk management that will be relevant to academicians for further research and for building the knowledge in the discipline.

### 1.8 Expected outcomes of the study

This research study sought to develop a model that would provide the following deliverables;

i. A model to help in determining the security risk exposure index in SACCOs

ii. Downloadable and/or printable recommendations that is helpful to the management of SACCOs for implementing necessary controls for safeguarding their business against risks.

iii. Appropriate data for SACCO regulatory authorities to aid in their oversight work of ensuring exposure in SACCOs to kept to minimum acceptable levels as possible.

### 1.9 Justification of the study

According to PWC report of the survey conducted in 2014 about "Threats to the financial services," financial sector has become a more attractive target than any other industry. 45 percent of reported economic crimes affected financial service providers in 2014 compared with 34 percent across all the other industries in the same period. Cybercrimes, which were also the focus of PWC study, noted that 39 percent of the cybercrimes targeted financial institution as compared to only 17 percent that were reported to affect other industries. In all these cases, financial institutions appear to be the prime targets of most threats ranging from economic to cyber-related. Bonnette (2003) agrees that financial institutions continue to become an attractive target to these threats due to the nature of their industry.

Other studies indicate that SACCOs have an edge over commercial banks because of their low lending rates and the fact that they are fast adopting electronic banking (Waswa, 2013;

Koduk, 2015). This has assisted the SACCOs to woo citizens into joining them and thus increasing their deposits. Other studies portray SACCOs as weaker targets than commercial banks in terms of information security (Kigen *et al.*, 2015). There is therefore a dire need to develop a feasible means to remedy the situation at hand. In this case a model to help the SACCOs to be informed on their current posture that concerns exposure to current and potential security risks and ways to counter losses resulting from successful breaches on confidentiality, integrity and availability (CIA) of SACCO assets.

### 1.10 Scope of the study

The study targeted to develop a model to determine the level of exposure to security threats within SACCOs in Kenya by computing the security exposure index. There are already attempts to measure exposure, which this research does not aim at overlap, but to improve. This study seeks to develop a model supported by a prototype that computes security exposure index.

### 1.11 Limitations of the study

Due to the sensitivity of the matters under study, savings and credit cooperative societies were not free to give out all the information that the researcher required for fear of being seen as they are exposed. However, the researcher used structured questionnaires and assured the respondents of the ethical considerations applicable in the study.

### 1.12 Scalability

The model was to be implemented in SACCOs in Kenya as a pilot environment. However, the study has the potential of being scaled to other organizations and to countries other than Kenya. This is possible because the final product is a web-based application, which supports distributed connections.

# CHAPTER TWO
# LITERATURE REVIEW

## 2.1 Introduction

This chapter presents reviews of literature about risk exposure factor among savings and credit cooperative societies, specifically on risk management, asset management, physical and environmental security, human resources security, system security, access controls and compliance. Moreover, the models, the gaps that this study sought to fill and two stages of conceptual framework for designing the model and for implementing the model respectively are part of the chapter.

## 2.2 Risks

The broad definition of risk according to Mehmood and Rafique (2010) is the potential for events to bring about losses or fluctuations in future income of the organization. Therefore, the concept of risk is always future oriented. According to SASRA (2015b), risk refers to the likelihood that the result of an action or event could bring undesirable impacts on a SACCOs' capital, earnings, or its viability. The idea of risk puts together three thoughts: it singles outs an event and joins its likelihood of occurrence with its possible impacts then inquires the following; what is the likelihood for that event happening in the future? What harmful effects would it have if it actually happened? An event with high risk, therefore, would have both a high likelihood of happening and a bigger negative impact if it happened. According to SASRA (2015b), a sound risk-management-program from any SACCO regardless of their size should include; risk tolerance, risk identification, risk management, risk control, and risk monitoring.

### 2.2.1 Risk Identification

Risk identification encompasses everything about understanding all the risks that make up the risk profile of an organization. It is a process that helps the organization to produce a comprehensive list of risks as well as opportunities and arrange them as per their risk categories, which are operational risks, compliance risks, strategic risks and financial risks (Curtis & Carey, 2012). The authors further suggested a risk assessment criterion, which incorporates: development of assessment criteria, actual assessment of risks, assessment of risk interactions, and prioritization of the risks by providing a balance between the level of risk and predetermined target tolerance thresholds and risk levels.

### 2.2.2 Risk Assessment

According to Curtis and Carey (2012), risk assessment entails the quantification and prioritization of risks for risk levels to be managed within established thresholds of tolerance. Risk assessment is very important because it helps organizations to know how big their risks are to focus their management attention in planning for appropriate responses to them. Figure 1 below demonstrates the risk assessment process.

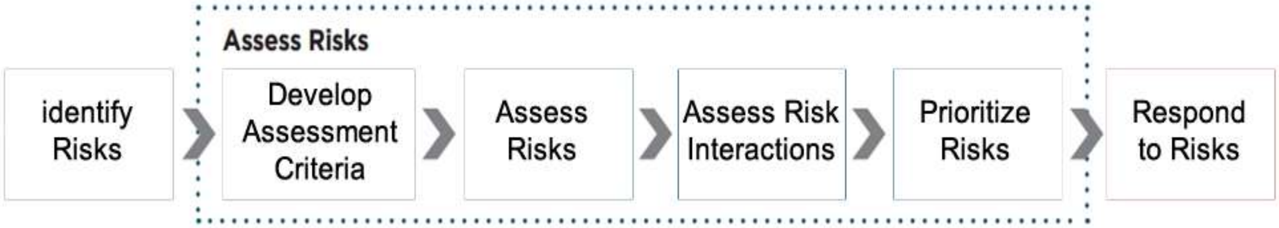


**Figure 1: Assess Risks Process**

**Source (Curtis & Carey, 2012)**

### 2.2.3 Risk Treatment

Risk treatment is the management strategy of response to each risk identified through risk assessment procedure. Risk treatment strategies include; acceptance, transfer, mitigation, or avoidance of risk. Clause 4.2.2.a of ISO 27001 (2005) standard requires that organization create a risk treatment plan as a living document to help in identifying the most appropriate actions, priorities and responsibilities of the management team.

### 2.2.4 Risk Owners

A risk owner is a person or entity that has the authority and is accountable for managing risk. They are usually the asset or service owners or departmental heads of organizations. Therefore, for each risk scenario, it is important for an organization to identify and record risk owner in the information security risk register (Oxford, 2015).

### 2.2.5 Components of Risks

Many formulas used for computing risk incorporate threats, vulnerabilities, likelihood, impacts, and controls as the main components of risk. However, according to Cole & Ring (2005), the most comprehensive formula for calculating risk as a function of threats, vulnerabilities, likelihood and countermeasures is as shown in equation 1 below;

$$\textbf{Risk} = \textbf{(threat x vulnerabilities x probability x impact)/countermeasures}$$

Equation 1: Risk measurement

In the view of the above, threat is considered as the component that drives the train in the formula for calculating risk. Chardantseva et al. (2016), on the other hand, provides a relationship between risks, threats, and impacts. The authors termed this as an accepted formula for calculating risks as shown in equation 2 below;

$$\mathbf{R=tvx_{tv}}$$

Equation 2: Accepted formula for risk

Where; ***t*** *is* threat, ***v*** *is the* vulnerability, and $\mathbf{x_{tv}}$ is the consequences/impact, and ***R*** is risk.

### 2.3 Assets Management

According to ISO/IEC 27001:2005 standard, an asset is “anything that has value to the organization.” Assets can be in form of electronic information, software, hardware, software, people, infrastructure, outsourced services, and other things that give value to the organization (Calder & Watkins, 2008). Together with threats and vulnerabilities, assets are key elements for risk identification. One of the fundamental concepts of ISO 27001 standard regarding assets is the need to assign owners to the assets so that the asset owners can be held responsible for use and protection of assets’ confidentiality, integrity, and availability (ISO 27001, 2005). According to ISO 27001 (2013), assets are managed because of two major reasons; one, assets together with threats and vulnerabilities are important recipes needed when performing risk assessment, and two, assets need to be assigned to asset owners who are responsible for acceptable use and safeguards for confidentiality, integrity, and availability of those assets.

### 2.3.1 Assets Owners

Asset owner is a person or a function that operates assets and therefore is answerable for the assets and information related to those assets by ensuring that they are protected from unauthorized access, use and modification (Calder & Watkins, 2008). Control A.7.1.2 from ISO 27001:2005 Annex A requires that an organization maintain in their Information Security Management System (ISMS); all their assets and have a nominated owner who is a member of staff who will be responsible for those assets. As an agreement to the ownership of asset, the nominated owners need to sign memoranda. The asset owner can entrust ownership of the asset to another owner who in turn become accountable for the assets. The importance of asset ownership is that it ensures proper management and protection of assets assigned to asset owners.

### 2.3.2 Assets Inventory

According to A.7.1.1 control of ISO 27001 standard, it is required that an inventory of all assets that are valuable to the organization must be drawn. In so doing, proper identification of assets must be done and full descriptions included which include the nominated asset owners. According to ISO 27002, the following categories of assets need to be known and maintained in the asset inventory; physical assets, software assets, information, people, services and other intangible assets such as reputation and brand (Calder & Watkins, 2008).

### 2.3.3 Acceptable use of Assets

According to control A.8.1.3 of ISO 27001 (2013), the organizations must document and implement the protocols for acceptable use of information assets, services, and systems by employees, contractors and other third parties. The particular focus here is on acceptable use policy on internet, mobile devices, emails and other information systems outside the confines of the organization.

### 2.3.4 Threats to Assets

A threat in information security is defined as anything that may occur or may not occur but if it occurs, it has the potential of causing harm to information and/or information system (Techopedia, 2016). NIST coined a definition for threat as a probability for a threat-source to take advantage of a vulnerability whereby vulnerability is a weakness in the system through which accidental or intentional exploitation can occur. (Goguen & Fringa, 2002). According to Kasyamu (2016), cyber threats are adversaries or actors that exhibit the strategic behaviour and capability to exploit cyberspace intending to hurt life, property, operations, information, and/or environment. Cruz (2013), argues that an enhanced definition for threat is; a possible cause of an undesired impact on a system or on an organization. It can further be categorized as either vulnerabilities or exposures.

As alluded by IPA management guide series (2013), serious security threats surrounds organizations and therefore organizations' attention must be drawn towards the prevention or mitigation strategies that would ensure that assets are safe. As eluded by Biscoe (2017), there are ten major threats that must be included in ISO 27001- risk assessment. They include; Social engineering, unauthorized access to networks, disclosure of passwords and restricted information, errors in maintenance, hardware theft, destruction of records, human or natural disasters, terrorist attacks, loss of electricity, and malfunctioning of equipment. The Insider Owing to the fact that threats exist, the Threat Spotlight Report of 2016 records that the valuable assets that organizations possess are at risk. Once threats exploit vulnerabilities, they either gain illegal access accidentally or intentionally, cause harm, or obliterate assets (Byres & Lowe, 2004).

Alberts and Dorofee (2003) presents a relationship that exists between information threats and what outcomes the relationship produces. According to the authors, there are four major classes of threats, namely; deliberate actions by people who can be insiders or outsiders; accidental actions by people from inside or outside the organization; system faults such as hardware crashes, and other events such as power cuts, fires and earthquakes. Their further argument alludes that the four categories of threats have the potential to produce four outcomes for each threat, namely; alteration, disclosure, obliteration or loss, and disruption of access. Figure 2 below demonstrates the relationship that exist between assets and threats and the outcome thereof (Open University, 2013)

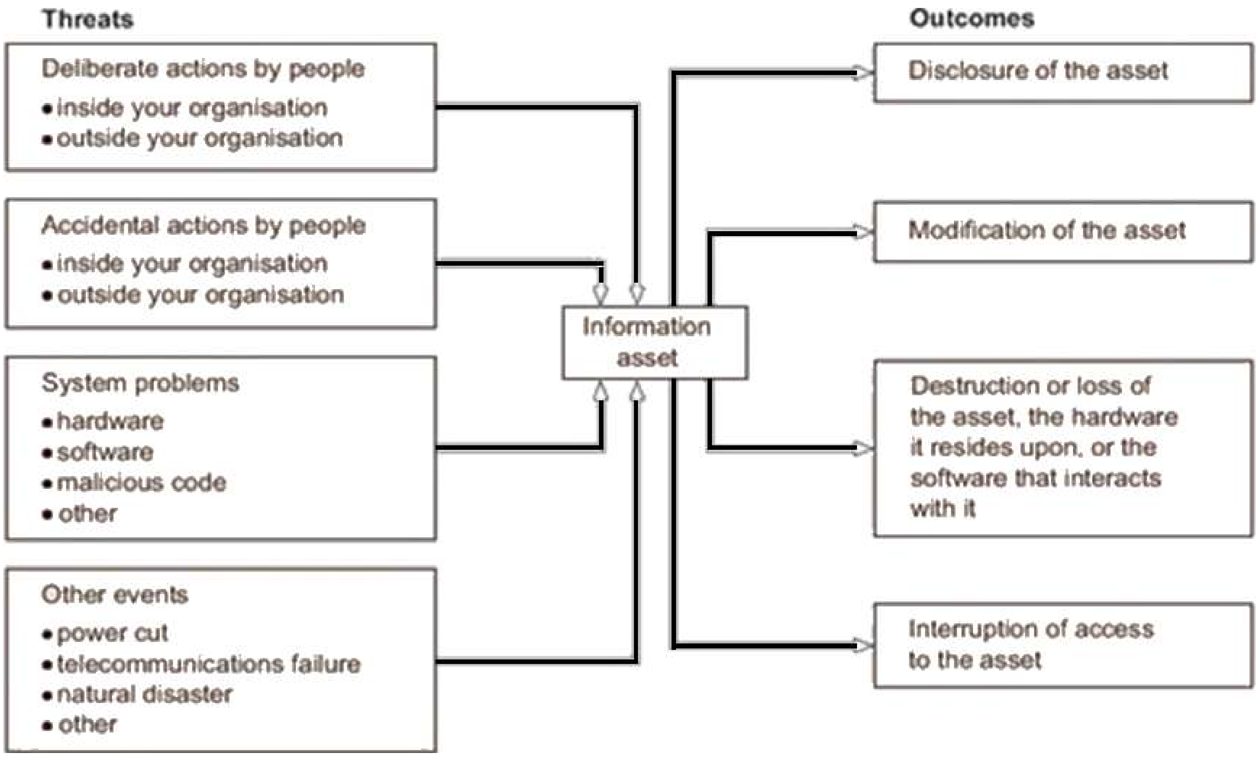

Threats
Deliberate actions by people
• inside your organisation
• outside your organisation
Accidental actions by people
• inside your organisation
• outside your organisation
System problems
• hardware
• software
• malicious code
• other
Other events
• power cut
• telecommunications failure
• natural disaster
• other
Information asset
Outcomes
Disclosure of the asset
Modification of the asset
Destruction or loss of the asset, the hardware it resides upon, or the software that interacts with it
Interruption of access to the asset

**Figure 1:** The relationship between assets, threats, and outcomes

Source :( Open University, 2013)

The present world of inter-connections present boundless opportunities and threats at the same time, therefore, it is important to consider what threats exist to assets in an organization once the information sets and their “owners” have been identified. It is therefore prudent to ensure that there are as secure applications and connections as possible (PwC, 2016). There are notable changes in threats from a time when threats were highly visible attacks by intruders driven by the search of notoriety, fame and glory to the present day threats which are largely invisible attacks driven by criminal motives and fraudulent desires (Bauer & Dutton, 2015). They continue to note that the threat landscape is so dynamic which means that the attempts to reduce the threats from one generation of attack vectors is bound to yield temporary success until new forms of threats emerge. Bradshaw (2015) agrees that there exists, sophisticated actors that create and deploy new techniques for every new threat.

### 2.3.5 Classification of threats

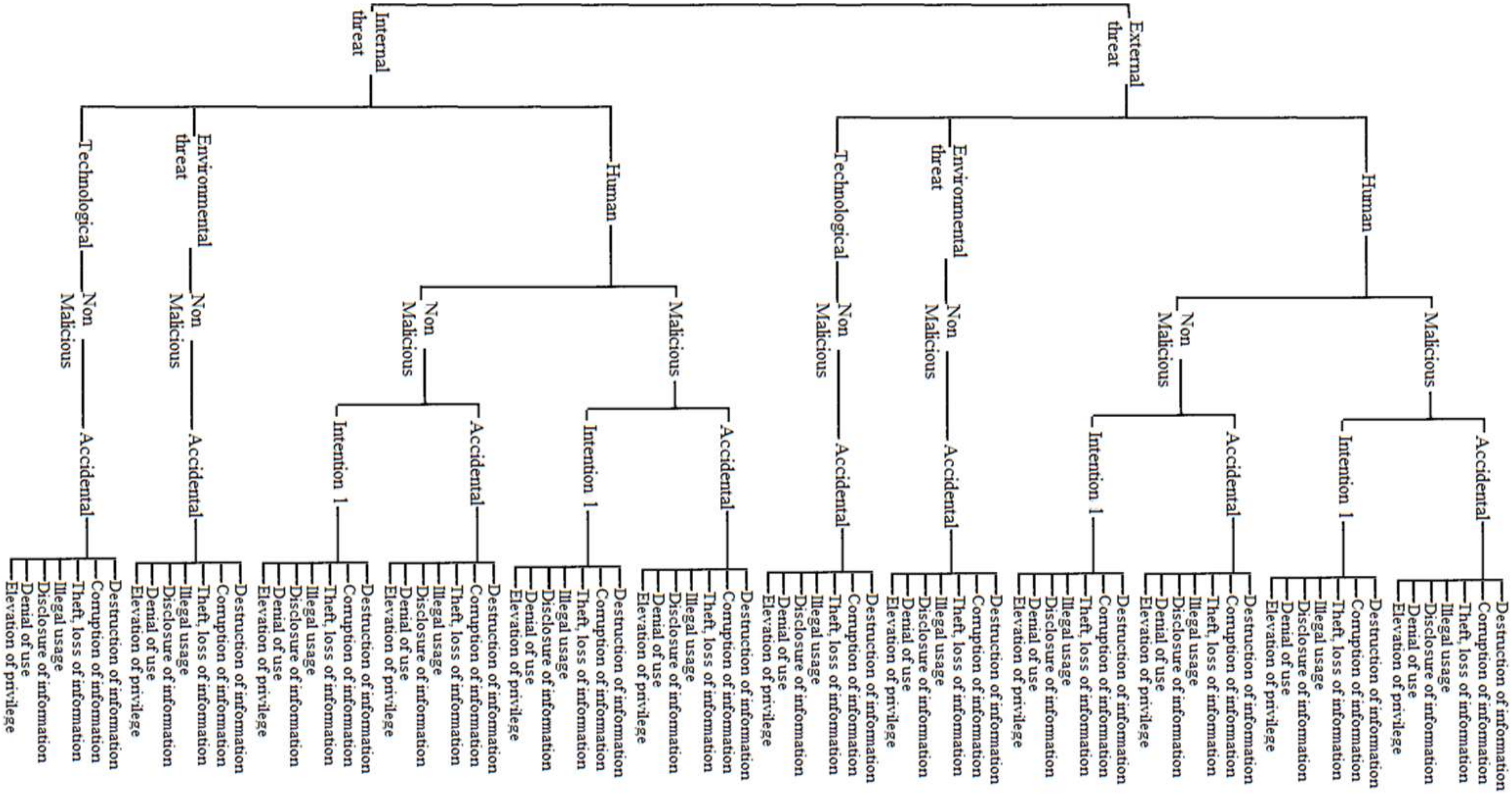
According to Jouini et al. (2014), proper classification of assets will allow identification and understanding of threats characteristics and source to protect systems assets. They argue that many organizations are victims to a number of threats that negatively affect their reputations and therefore it is prudent for the organizations to identify all threats characteristics in order to mitigate their risks. Many research works have developed numerous ways in which threat can be classified. Some base their classification of threats on the origin of threats, motive of the threat and its nature. In a broader perspective, there are two types of threats, namely; internal and external threats. Internal threats emanate from inside the organization while external threats emanate from outside of the organization (Verizon, 2016). Considered from another dimension of motive, threats can be classified broadly as either intentional or accidental.

Diaz-Gomez et al. (2010) termed the threats as penetrations. They argue that external penetrations are considered from the perspective of access to computer, its programs or data and not necessarily coming from outside of the organization. They are instead employees or contractors who have no access to computer resources or data. They further claim that internal penetrations are attackers who have access to the computer but are not authorized to access certain data or programs within the computer. In as much as there are outsider and insider threats to worry about, latest trends portray that a worrying 70% of the total information security threats emanate from within an organization. However, this trend is expected to further increase because of the present opportunities for mobility through the discovery of portable devices such as laptops, smart phones and ipads (Sugata *et al*., 2010).

According to Franqueira et al. (2010), there are particular attributes for the insider threats as well as for the outsider threat. By their definition, outsiders are persons who are untrustworthy and therefore do not have any authorized permissions to access organization’s asset. Outsiders are attributed with mistrust and unauthorized access. Insiders, however, are persons who are trusted and therefore have some authorized permissions to access organization’s assets. Insiders are attributed with trust, authorized access, legitimate privileges, knowledge, organizational controls, and perception of risks. Further, there is another group called external insiders that are neither insiders nor outsiders but fall somewhere in between a set of insiders and a set of outsiders (Franqueira *et al*., 2010). They are persons that are not trusted but have some authorized permission to access the organization's assets. The attributes of external insiders include; mistrust, authorized access and organizational controls.

In accordance with Bonnette (2003), threats are categorized broadly as either human or non-human or a hybrid of both. Human threats are threats that are perpetrated by people who can be individuals from inside the organization, persons from outside the organization, or a collaboration of both insiders and outsiders. They have particular names that define them such as; hackers, crackers, insiders, partners, competitors, or terrorists. Non-human threats comprise all types of natural disasters, which include; floods, fires, earthquakes, hurricanes, tornados and severe storms. Mixed threats are a hybrid of both human and non-human threat sources. Humans originally create them but take their own life once they are released. Examples of these mixed threats include malicious code such as warms, Trojan horses, viruses, and malware. Furthermore, Rufi (2007) added to the argument of humans as threats by claiming that threats are just but humans who are eager, willing and qualified to exploit any security weakness by continually searching for new exploits and weaknesses, which in other terms is referred to as vulnerabilities.

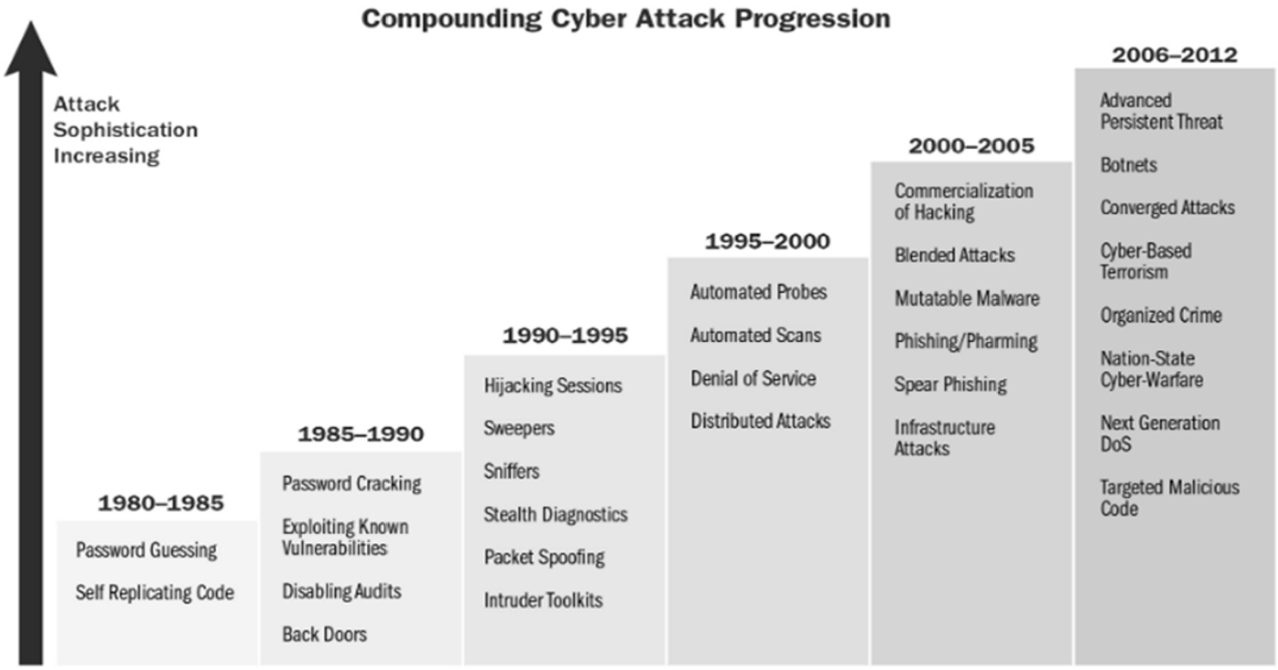
Jouini et al. (2014), proposed a comprehensive hybrid model for classification of threats, which they termed as Multi-dimensions model for threat classification. They argue that other researchers have failed to provide exhaustive list and categorization of threats and therefore the main idea behind their model is to combine several classification criteria proposed by others and present their potential impact. Multi-dimensions model of classification classify threats basing on their source, threat agents, threat motivation, threat intention and the impact as presented in the figure 3 below.


Internal threat
Technological
Non Malicious
Accidental
Destruction of information
Corruption of information
Theft, loss of information
Illegal usage
Disclosure of information
Denial of use
Elevation of privilege
Environmental threat
Non Malicious
Accidental
Destruction of information
Corruption of information
Theft, loss of information
Illegal usage
Disclosure of information
Denial of use
Elevation of privilege
Human
Non Malicious
Intention 1
Destruction of information
Corruption of information
Theft, loss of information
Illegal usage
Disclosure of information
Denial of use
Elevation of privilege
Accidental
Destruction of information
Corruption of information
Theft, loss of information
Illegal usage
Disclosure of information
Denial of use
Elevation of privilege
Malicious
Intention 1
Destruction of information
Corruption of information
Theft, loss of information
Illegal usage
Disclosure of information
Denial of use
Elevation of privilege
Accidental
Destruction of information
Corruption of information
Theft, loss of information
Illegal usage
Disclosure of information
Denial of use
Elevation of privilege
External threat
Technological
Non Malicious
Accidental
Destruction of information
Corruption of information
Theft, loss of information
Illegal usage
Disclosure of information
Denial of use
Elevation of privilege
Environmental threat
Non Malicious
Accidental
Destruction of information
Corruption of information
Theft, loss of information
Illegal usage
Disclosure of information
Denial of use
Elevation of privilege
Human
Non Malicious
Intention 1
Destruction of information
Corruption of information
Theft, loss of information
Illegal usage
Disclosure of information
Denial of use
Elevation of privilege
Accidental
Destruction of information
Corruption of information
Theft, loss of information
Illegal usage
Disclosure of information
Denial of use
Elevation of privilege
Malicious
Intention 1
Destruction of information
Corruption of information
Theft, loss of information
Illegal usage
Disclosure of information
Denial of use
Elevation of privilege
Accidental
Destruction of information
Corruption of information
Theft, loss of information
Illegal usage
Disclosure of information
Denial of use
Elevation of privilege

According to Nyawanga (2015), other information security threats include piracy, breaches of personal privacy, computer viruses, industrial espionage, cyber terrorism, e-mail spam and electronic warfare. These threats, according to Nyawanga, cannot be overestimated and they could have awful consequences on the critical information infrastructure of any country.

### 2.3.6 Threat Landscape

According to KPMG (2016), the embracing of upcoming technologies has exposed the organizations to the developing and rising landscape of cyber threats and vulnerabilities. According to the government of Kenya cyber security strategy (2014), Kenya faces an increasingly evolving cyber threat landscape like any other nation with robust ICT infrastructure as it matures into an information society. There has been compounding progression on the sophistication of cyber-attack in Kenya between 1980 and 2012 according to the Kenyan government cyber security strategy. PWC (2016) in their Global Economic Crime Survey report agrees that cyber threats continue to increase but organizations' preparation is not keeping the pace. Figure 4 below depicts a cyber-threat landscape in Kenya.



### 2.4 Physical and Environmental Security

Control 9 of ISO 27001 manages physical and environmental security and its main objective is to avert unauthorized persons from access, damage and interference organization's physical location as well as information (ISO 27001:2013). According to Henage and Henage (2013), unauthorized persons achieve physical security through installation of physical access barriers whereby a physical access barrier is any physical construction that hinders or limits access to organizations valuable assets. Physical barriers may include locks on doors. However, the extent of sophistication of the physic barrier directly depends upon the value of the assets. Physical and environmental security, according to ISO 27001 (2013), is broadly classified into two classes, namely; secure areas and equipment security that are recorded as control A.9.1 and control A.9.2 respectively.

#### 2.4.1 Secure Areas

The primary objective of this control is the protection of organization's working areas, locations or information from physical access, interference, or damage by unauthorized persons. To achieve this control's objective, the control is guided by six sub-clauses denoted as control A.9.1.1 to control A.9.1.6. The sub classes are; physical perimeter security that require organizations to safeguard areas that contain information and information facilities by use of such barriers as walls and operated gates. Physical entry controls that require organization to protect their information and facilities containing information using sufficient access controls to make certain that only authorized persons are permitted access. Secure rooms, offices and facilities that prompt institutions to design and apply physical security to rooms, facilities and offices. protection against damages occasioned by external and environmental threats which are either natural or man-made; Design and application of physical guidelines and protection for working in secure areas; and control and isolation of public access, delivery and loading areas to avoid unlawful access.

#### 2.4.2 Equipment Security

Control A.9.2 of the standard addresses the security of organization's equipment. It requires that organizations should protect their assets from damage, loss, compromise or theft and disruption of activities resulting from such breaches. The control is further broken down into seven sub-clauses denoted as A.9.2.1 to A.9.2.7 in order to exhaust the aspects of equipment security and disposal (Calder & Watkins, 2008).

### 2.4.2.1 Equipment Siting and protection

This is addressed in Control A.9.2.1 that requires the organizations to site or protect the equipment to reduce the risks from unauthorized access, hazards, and environmental threats. According to ISO 27002, a number of controls need consideration while siting equipment to ensure they are well protected. They include; situating equipment in places that are free from unnecessary interference or access by persons without permission. Storage and information processing facilities bearing sensitive information should not be positioned in such a way that passers-by can overlook. Items that require exceptional protection needs isolation in order to reduce the risk of damage, loss, interference or compromise; ISO 27002 also recommends that organizations should reconsider their internal policies about smoking, drinking or eating within the proximity of information processing equipment; the organizations should also consider the dangers of information leakage (Calder & Watkins, 2008).

### 2.4.2.2 Supporting Utilities

This control is captured as control A.9.2.2 and it requires that organizations should protect their equipment from disruptions and anomalies in electricity supply and other supporting utilities. To ensure that there is appropriate protection of equipment from failure of supporting utilities; organizations should hire services of qualified engineers to have a *Rota* of regular inspection to ensure that those utilities are in proper working conditions and will continue to work. In addition, it is prudent for organizations to install uninterrupted power supply systems (UPS) and back-up power generators to support equipment that run critical business applications (Calder & Watkins, 2008).

### 2.4.2.3 Cable Security

Control A.9.2.3 of the ISO 27001 standard calls for organizations to protect power cables and telecommunication cables transmitting data from interference, interception or damage. On the same issue, ISO 27002 standard recommends the following to be put in place in order to have secure cables; power and telecommunication cables should be put underground, on secure ducts or alternative secure protection. Cables in the working area should be properly and adequately organized and managed since cables lying on the floors are highly vulnerable to breakages; power cables and communication cables should be separated to prevent interference; network cables should be protected using conduits.

#### 2.4.2.4 Equipment Maintenance

Control A.9.2.4 of the standard necessitates the organizations to maintain equipment to ensure it continually remains available and its integrity is protected. This means that the organization should maintain its information processing equipment in working order according to the manufacturer's instructions and only authorized trained personnel (Calder & Watkins, 2008) must carry out repairs and maintenance procedures.

#### 2.4.2.5 Security of equipment off-premises

Working outside the organization's premises is often times risky; therefore, control A.9.2.5 of the ISO 27001 standard necessitates the organizations to incorporate security to off-site equipment as well. According to Calder & Watkins (2008), off-site use of any equipment such as laptops, line management must approve mobile phones, notebooks and personal digital adapters (PDAs). According to ISO 27002 standard, the following controls needs consideration to make certain security of equipment off-premises; equipment used outside the organization's premises should not be left unattended; staff responsible for use of the equipment outside the premises should be trained about the risks identified by the manufacturer and recorded on the instruction manuals.

#### 2.4.2.6 Secure disposal or reuse of equipment

According to this control, organizations should check to ensure that storage media and all other items of equipment that can store licensed software and sensitive data have been erased or securely overwritten before disposal. According to Calder & Watkins (2008), it is better to destroy such media than to reuse; for instance, destroy the hard disk of the PC before selling it off.

#### 2.4.2.7 Removal of property

According to ISO 27001 standard's control A.9.2.7, any information, equipment, or software removed from the organization's premises must be authorized; that is to say, no equipment, software or information should be removed from the premises without authorization. In addition, there should be appropriate controls to ensure that portable devices in the possession of the staff should be recovered before they leave the organization and proper spot checks should be put in place to ensure that no property leaves the premises without approval.

## 2.5 System Security

Control A.12 of ISO 27001(2013) standard centers on guidelines for system security, namely; purchase, development, and maintenance of information systems to be used in the organization. This control focuses on ensuring that security is built into information system as an integral part.

### 2.5.1 Security requirements of information systems

According to Calder and Watkins (2008), the main objective of system requirements of information systems control is ensuring that security becomes the fundamental part of information systems. It requires that organization should analyze and specify their security requirements for new information system or for enhancement information systems (that already exist) with security controls.

### 2.5.2 Correct processing in applications

This control denoted in ISO 27001 standards as Control A.12.2 is focused at preventing errors, loss, unauthorized alteration or mishandling of information in applications. It is further broken down into four sub-controls denoted as Control A.12.2.1 to Control A.12.2.4 as follows; Input data validation to authenticate that the data being keyed into the applications is appropriate and correct. Control of internal processing which ensures that validation checks are applied to detect any corruption of information occasioned by human purposeful acts or errors during processing. Message integrity for assuring that there is protection of message integrity and authenticity in applications and appropriate controls thereof, and output data validation for ensuring that the output from applications under any circumstances is correct and appropriate.

### 2.5.3 Cryptographic Controls

This control A.12.3 of the standard ensures that the confidentiality, integrity, and availability of information are protected using cryptographic means. It has two sub-controls, namely; policy to guide the use of cryptographic controls to ensure that the policies that protect information using cryptographic means is developed and implemented, and key management control that support the use of cryptographic techniques in the organization.

### 2.5.4 Security of System files

The intention of this control (A.12.4) is ensuring that security of system files is preserved. It is further broken down into three sub-controls, namely; protection of system test data that assures that there is careful selection, protection, and control of test data, control of operational software that assures that there are procedures to control installation of software on operational systems, and access control to program source code.

### 2.5.5 Security in development and support processes

This control A.12.5 aims at preserving the security of information and application system software. It is further classified into five sub-controls, namely; Post operating system changes technical review of applications, Information leakage, Software packages change restrictions, Change control procedures, and Outsourced software development controls.

### 2.5.6 Technical Vulnerability Management

This control (Control A.12.6) aims at decreasing the risks that results from exploitation of technical vulnerabilities in print. Specifically, it prompts organizations to obtain information pertaining technical vulnerabilities of information systems in a timely manner.

## 2.6 Human Resource Security

Employees, contractors and people within an organization are the greatest assets to that organization because of the value they bring in. However, they are considered the weakest link in information security (Bulgurcu *et al*., 2010). According to ISO 27001's control 8; human resource security is most important because the security of information in any organization is the responsibility of the employees and other people within that organization. Although some security threats and breaches are as a result of non-human factors, most of these threats and breaches are widely propagated by humans either accidentally or maliciously (Brauch, 2011). The Information Security management is focused on technology, processes, and people. However, many organizations put a lot of emphasis on securing processes and technologies, therefore disregarding people's security. Information security therefore is also a human challenge, which implies that people that develop the culture of the organization and are therefore custodians of security (Ashenden, 2008).

Recent research indicates that insiders who included employees of organizations perpetrated over 80% of system-related theft and fraud in Kenya.  The report continues to portray that in 2016 alone, 50% of direct costs of cybercrime were attributed to insider threats (Kigen *et al.*, 2016). In as much as the people are seen to be the main perpetrators of security breaches, employees and other people within organizations can be targets in the event, for instance, KPMG Cyber Crime Survey of 2015 indicates that 64 per cent of security breaches in many organizations target senior management and directors.  The main objective of ISO 27001's control 8 is to set rules and baseline requirements that organizations can apply before, during, and after change or termination of employment for all the employees hired or contracted by the organization.

### 2.6.1 Prior to employment

Pre-employment security issues captured in Control A.8.1 of the standard aims at ensuring that the most suitable candidates are hired for the job and that they understand their responsibilities in accordance with ISMS and information security in the organization (Calder & Watkins, 2008). In this case, the organizations are required to do thorough screening of the candidates being considered for the position by verifying their background according to applicable ethics, laws, and other regulations, perceived risks relative to requirements of the business, and the categorization of the information to be accessed. In addition, the control requires that the candidates being considered must agree to the terms and conditions of employment by signing non-disclosure agreements where they will be working with sensitive organizational information.

### 2.6.2 During employment

Control A.8.2 of ISO standard applies to employees, contractors and other users who work to bring value to the organization and the period during which they serve in those organizations. This ensures that all hired contractors and employees are conscious of their security responsibilities and are able to implement them. The main objective of this control is to ensure that all the contractors, employees and other third party users are informed about information security threats and are fully facilitated to support the organization’s security policy in their regular operation by reducing the risk of human error. In the event, all the concerned must strictly comply with the organizational laid down policies and procedures.

The organization is therefore required to focus security awareness and training on the entire user population with the management setting precedence for suitable IT security behavior within an organization. Efficient education, awareness and training programs on information and information system security should be established in all levels of the organization and should act as a basis for official disciplinary process for contractors, employees and other third party users who breach security (Wilson & Hash, 2003).

### 2.6.3 Termination or change of employment

The primary intention of this control is to assure those contractors, employees and other third party users leave or change employment in an organized manner. In this case, the responsibilities for changing employment or terminating concerned contractors or employees are well defined and assigned. At the point of termination of contract, employment, or agreement, the affected contractors, employees, or other third party users are required to return organization’s assets, which they possess. In addition, the access rights and permissions for which the employees or contractors were assigned needs to be revoked upon termination or changed appropriately if the affected persons are changing employment terms (ISO 27001, 2013).

### 2.7 Access Controls

According to Cruz (2013), lack of appropriate access controls leads to exposure of organization's assets to potential threats. The author defines exposures as system configuration issues or mistakes in software, which allow access to information or act as a springboard for hackers to gain access to a network or a system. Cruz further outlines the attributes of exposure to systems or organizations as able to allow attackers to collect system information. Able to allow attackers to hide traces of their activities, able to include capabilities that can be easily compromised even though their behavior was expected, the primary entry point for attackers to gain access to systems or organizations, and that exposure is a big problem according to reasonable security policies.

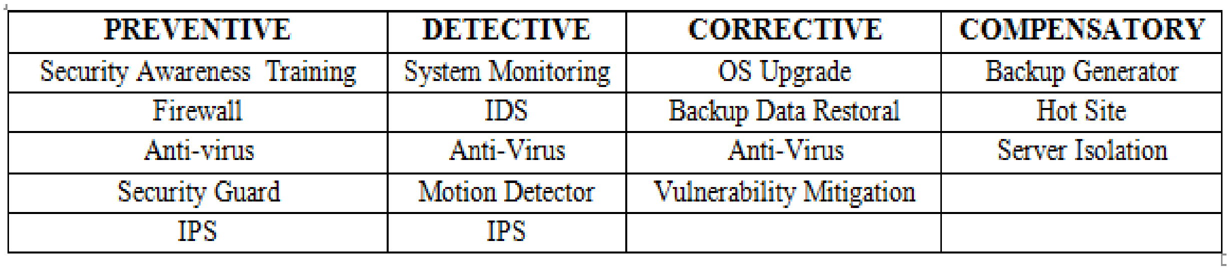
According to SASRA (2015b), the Sacco's board of directors and top management ought to implement robust internal control system to ensure that it is unduly exposed to threats. These internal controls are necessary to guarantee that; The Sacco's organizational framework sets up comprehensible outlines of authority, The Sacco's systems and arrangements offers business continuity planning, and the process of introduction and assessment strategic plans is all-inclusive and is held on to.

According to Northcutt (2009), the definition for Security access controls is; administrative or technical countermeasures or safeguards meant to avoid, counter, or decrease loss or inaccessibility occasioned by threats acting on their corresponding vulnerabilities. These security access controls are categorized into three; physical controls, technical controls and administrative or process controls. Physical controls refer to all physical deterrents and barricades that control access, for instance, lock and keys, and video surveillance systems. Technical controls refer to systems and software used to control access, for example, antivirus software and firewalls. Administrative controls on the other hand, refer to established policies, procedures, laws, guidelines and practices that regulate access to information and information systems (Tipton & Nozaki, 2012).

Further, Northcutt (2009) argues that security controls can be classified based on the phase of activities involved in implementing them and the purposes for which they are implemented.

The classification includes; preventive controls, detective controls and corrective controls. Preventative controls are implemented to thwart threats from exploiting vulnerabilities. Detective controls are implemented to identify threat that land in organizations' information systems. Corrective controls on the other hand are implemented to tone down or reduce the outcomes of the threat being manifested. When the environment limits the implementation of activity phase controls or that the activity phase controls fail to operate or are unavailable for use, Northcutt suggest an alternative set of controls, which organizations can implement. He terms these set of controls as compensatory controls and they include; implementation of backup generators, hot sites, and server isolation. Table 1 below illustrate activity phase of controls.

**Table 2.1: Illustration of Activity phased Control**



| PREVENTIVE | DETECTIVE | CORRECTIVE | COMPENSATORY |
|---|---|---|---|
| Security Awareness Training | System Monitoring | OS Upgrade | Backup Generator |
| Firewall | IDS | Backup Data Restoral | Hot Site |
| Anti-virus | Anti-Virus | Anti-Virus | Server Isolation |
| Security Guard | Motion Detector | Vulnerability Mitigation | |
| IPS | IPS | | |

**Source: Northcutt (2009)**

According to ISO 27001 (2013), access controls as the name suggests are mechanisms that protect information and information systems from being accessed by unauthorized persons. This control is presented in ISO 27001 asl A.11 and its primary intention is to manage how the information is accessed. It is further subdivided into seven sub-clauses denoted as A.11.1 to A.11.7 namely; user responsibilities, operating system access control, business requirenments for access control, application and information access control, user access management, network access control, and mobile computing and teleworking.The following is a review of each of the clauses.

### 2.7.1 Business requirement for access control

The focus of this clause is access control policy based on the current business needs of the organization. The organization's documentation and review of access control policies is driven by the business requirements of that organization. Both physical and logical access controls should be defined by the organization and should complement each other rather than conflict (Calder & Watkins, 2008). According to ISO 27002, access control policy of ISMS considers the following factors, namely; different business applications have different business requirements that define who should be allowed access. some information needed for some business applications could be processed by persons who do not need-to-know the application, user privileges should concur with the level of information that the user should access, relevant legislations must be analyzed while establishing a security policy and employee privileges should be revoked or changed when the employee is terminated or changes employment.

### 2.7.2 User Access Management

This control is captured as Control A.11.2 in ISO 27001 standard. Its focus is on the users and requires the organizations to ensure that only the users who are authorized are the only ones who can access the information systems and block any other users who are not authorized. It is further broken down into four sub-clauses, namely, user registration that requires establishment of an official registration and deregistration procedure for granting or revoking users' access. Privilege management that require organizations to restrict and manage the provision and use of access rights, management of user passwords which prompts organizations to have a formal management process for controlling the allocation of passwords, and review of user access rights that require that management in the organizations apply formal process to appraise user access rights on regular basis.

### 2.7.3 User Responsibilities

The main objective of this control (captured as Control A.11.3 in ISO 27001 standard)is to stop users who are not permitted access. It also prevents theft or compromise of information and information processing facilities. It contains three sub-controls, namely; password use that requires users to select and use passwords based on good security practices, unattended user equipment that require all users to appropriately protect all the unattended equipment within the organization, and clear screen and desk policies that requires employees to clear all papers and removable storage media as well as accessible computer screens.

### 2.7.4 Network Access Conrol

The main purpose of this control is to protect networked services by preventing unauthorized access to them. According to ISO 27001 (2013), the network access control is further broken down into seven sub-controls to exhaust protection of networked services. The sub-controls include; policy on-use of network services which prompts organizations to ensure that users can only gain access to specific network services for which they have authority to use. Proper authentication of users to manage how users connect to services remotely, remote analytics and configuration. Identification of equipment in networks whose primary function is to ensure that there is an automatic identification as a means through which connections from definite sites and equipment are authenticated. Port protection that ensures that physical and logical access to diagnostic and configuration ports is controlled, segregation in networks for segregating information systems, groups of information services, and users, network connection control to restrict connections in shared networks, and network routing control that assures that information flows and no computer connections infringe any access control policy of business applications.

### 2.7.5 Operating System Access Control

The main purpose of this clause (A.11.5) is to stop any unauthorized access to operating systems. It is further broken down into six sub-controls (control A.11.5.1 to control A.11.5.6) in the ISO 27001 standard to ensure exhaustive protection of operating systems. The sub-controls include; secure log-on processes that assure that access to the operating system is controlled. User identification and authentication using unique user ID and secure authentication password management system that is interactive to ensure quality passwords are used. System utilities to ensure restriction and strict control of utility programs that are capable of overriding systems and applications, session time-out to shut down inactive sessions if inactive for a specified period, and restriction of connection time to give supplementary security for high-risk applications.

### 2.7.6 Application and Information Access Control

The purpose of this clause (A.11.6) is to stop unauthorized access to information within application systems. It has two sub-controls, namely; information access restraint to limit access to information and application systems by users and support personnel based on definite access control policy, and sensitive information isolation that require that sensitive information shall have dedicated computing environment.

### 2.7.7 Mobile Computing and Teleworking

This is ISO 27001 standard control A.11.7 that aims to assure information security when using mobile computing and teleworking facilities. The control has two sub-controls, namely; mobile computing and communications control that require adoption of formal policy and suitable security procedures to guard against risk of using communication facilities and mobile computing, and teleworking control that require policies, operational plans and procedures to be developed and implemented for teleworking activities

## 2.8 Compliance

The generic definition for compliance is the conformity to fulfill the official requirements whereas the definition for security compliance is the state of conforming to security requirements that are imposed externally and of giving proof (assurance) there of (Julisch, 2009). Compliance management, on the other hand is the procedure through which organizations deals with the entire compliance process from the onset (Chatzipoulidis & Mavridis, 2009).

According to Calder and Watkins (2008), this control is aimed at ensuring that the organization does not violate any civil or criminal law, as well as any contractual, statutory or regulatory obligations, and any other security needs. The control on compliance is captured in ISO 27001 standard as control A.15. It has three sub-controls denoted as control A.15.1 to control A.15.3, namely; technical compliance, legal requirements compliance, security policies and standards compliance, and information systems audit considerations. The following is a detailed presentation of the sub clauses.

### 2.8.1 Compliance with legal requirements

The objective of this control A.15.1 of ISO 27001 standards is the requirement that the organizations should avoid breaching any contractual, statutory, or regulatory obligations. It has a total of six clauses that help the organizations to avoid any breaches of the law, namely; Identification of applicable legislation that require the organizations to define, document and keep update of regulatory, contractual and statutory requirements. The organizational approach to meet them, Intellectual property rights control that necessitates organizations to implement proper procedures for ensuring that they are compliant with regulatory, contractual and legislative requirements pertaining the use of proprietary software.

The following are other clauses under this control; protection of organizational records that requires organizations to comply with contractual, statutory, regulatory and business requirements by protecting their records from loss, falsification and destruction. Protection of data and privacy of personal information clause that necessitates organizations to comply with applicable regulations, legislations, and contractual clauses by making sure that there is protection of data and privacy. Prevention of misuse of information processing facilities clause that require organizations to deter their users from using information processing facilities for unlawful purposes; and regulation of cryptographic controls clause which necessitates organizations to comply with all applicable regulations, agreements and laws while using cryptographic controls.

### 2.8.2 Compliance with security policies and standards, and technical compliance

The purpose of this clause A.15.2 is to ensure that systems comply with organizational security policies and standards. It has two clauses, A.15.2.1 and A.15.2.2, namely; Compliance with security standards and policies, which oblige managers of organizations to comply with security policies and standards while carrying out all their security actions within their area of duty; and technical compliance checking that entails regular checking of information systems to ascertain that security implementation standards are complied with.

### 2.8.3 Information systems audit considerations

The purpose of this control A.15.3 is to ensure that effectiveness is maximized while there is minimum interference to/from the information systems audit process. It has two clauses, A.15.3.1 and A.15.3.2, namely; Information systems audit controls to ensure careful planning and agreement to ensure minimum disruption to business processes during audit and checks on operational systems; and protection of information systems audit tools to put off any potential misuse or compromise to protect access to information systems audit tools.

### 2.9 Existing models for determining Risk Exposure

The informal definition of a model according to Mateski et al. (2012) is a simplified representation of something else by ignoring, masking, or abstracting unnecessary details and instead highlighting the details of interest. A security model in computing is a design for identifying and implementing security policies and may be instituted upon formal models, which include access privileges, a computational model, and a distributed computing model (Krutz & Vines, 2003).

#### 2.9.1 ISO/27001 Standard

The International Organization for Standardization (ISO) and the International Electro-technical Commission (IEC) are the two international bodies that formulate standards for best practice in different fields worldwide. The Joint technical committees (JTC1) of these two bodies work together in areas of reciprocal interest (Schweizerische, 2013). ISO 27001 is an international standard that was published in 2005 as ISO 27001: 2005 and revised in 2013 by the JTC as ISO 27001: 2013. The ISO 27001 standard was developed to provide protection to the assets in the organization and therefore it is a good starting point when developing information security (Fomin *et al.*, 2008).

According to Brewer and Nash (2010), the standard outlines the requirements that are necessary to establish, implement, maintain, and continually improve Information Security Management system (ISMS). The standard is applicable to all forms of organizations ranging from government agencies, to commercial enterprises, to non-profit organizations. The purpose of the ISMS is to provide tools, processes, and ways of working in order to improve the level of information security within organizations that implement it. The standard contains actual requirements part and an annex, Annex A, which catalogues a set of 133 controls from which an organization can choose what is applicable to them for securing their information assets. The choice of controls and other relevant measures by the organization is based on the security requirements and necessary controls identified by risk assessment process (ISO

27001 Annex A, 2017). This is done through a process called Statement of Applicability (SOA). Figure 5 below shows the cross-checking process used for selecting and implementing controls to meet the organizations' needs for controls identified by risk assessment and risk treatment.

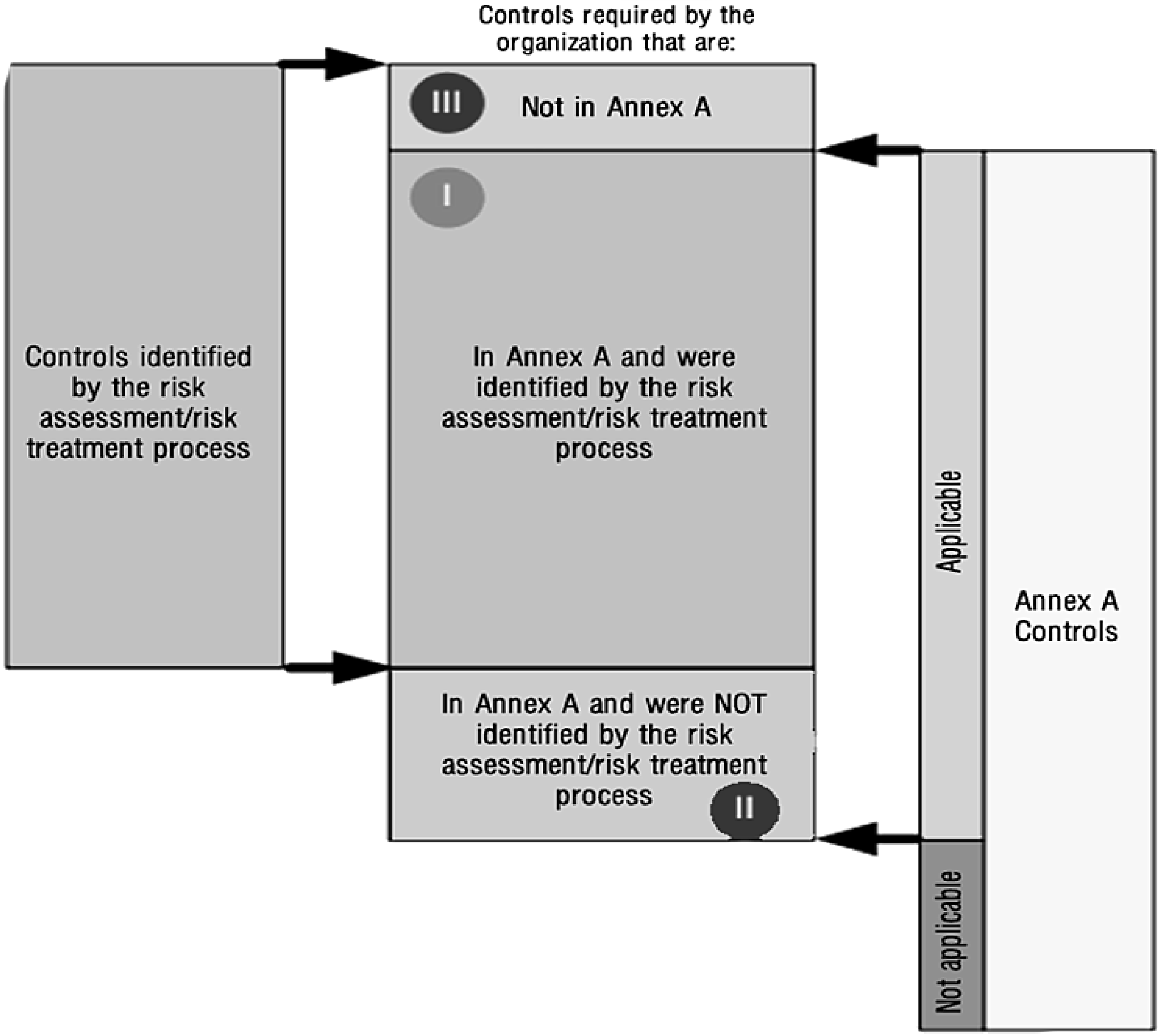

Controls required by the organization that are:
III
Not in Annex A
I
Controls identified by the risk assessment/risk treatment process
In Annex A and were identified by the risk assessment/risk treatment process
In Annex A and were NOT identified by the risk assessment/risk treatment process
II
Applicable
Not applicable
Annex A Controls

**Figure 4:** ISO27001 Annex A Crosschecking Process.

**Source (**Brewer & Nash, 2010**)**

According to Susanto et al. (2012), ISO 27001 acts as a general management and control framework that helps organizations to manage their information security risks. With ISO/IEC standard, any organization can set up a security procedure, which steadily optimizes the security in that organization to an identifiable level. It has numerous advantages for the organization that implement, namely; it acts as a confirmation of organizations security to third parties. An independent authority documents it; therefore, it adds competitive advantage. It reduces cost through optimized, transparent structures. It enables organizations to adopt security as their essential element of business processes. It allows for knowledge and monitoring of residual IT risks and other IT. It enables structures and processes to be documented properly, it helps increase security awareness of the employees, it allows for appraisal of the organization's processes from security standpoint, it enables organizations to prioritize the security of their operations and therefore assures that business continuity is managed, it is a standard with global recognition.

### 2.9.2 Process approach of developing ISMS

According to Nakrem (2007), "process approach" is the organizational use of a set of processes, together with the recognition and relations of these processes and their management. The process approach model also referred to as ISMS cycle is a presentation of continuous phases to establish, implement, monitor and review, and maintain and improve ISMS. ISO 27001 standard presents a process approach for managing information security that encourages users to apply Plan, do, check, and act (PDCA) process during implementation of ISMS in the organization.  Figure 6 below shows the PDCA process for building effective ISMS for an organization.

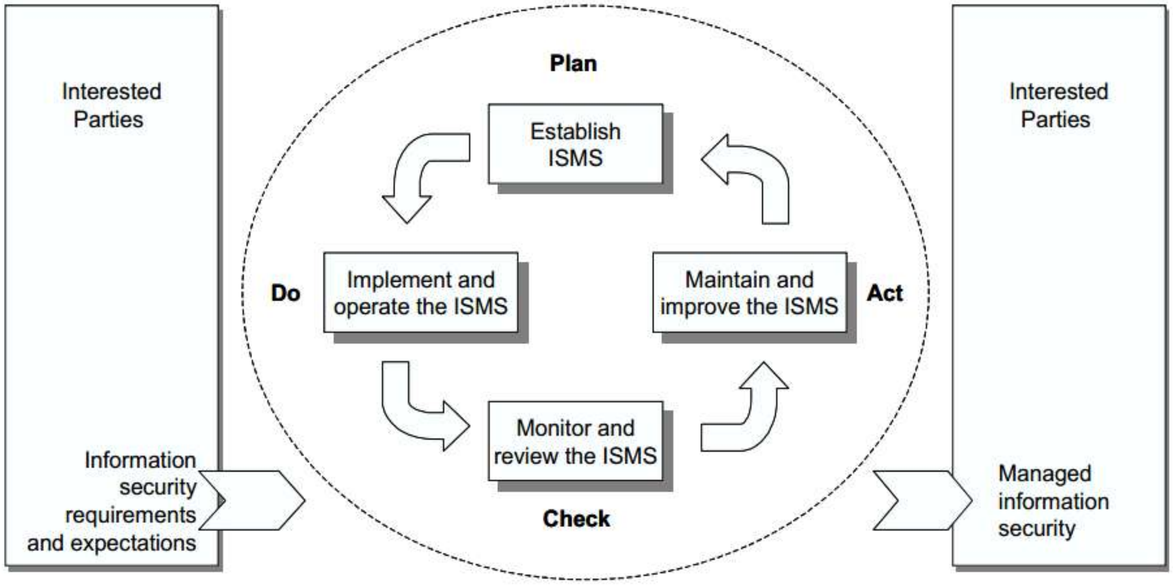


**Figure 5: PDCA model for building ISMS**

**Source: (ISO 27001, 2005)**

Where;

**Plan:** Means to identify information assets and to understand organization's information security requirements. Assess information security risks and select controls to manage unacceptable risks.

**Do:** refers to implementing controls and managing operations.

**Check:** refers to monitoring and reviewing the performance and effectiveness of the information security system

**Act:** relates to application of preventive and corrective actions on continuous basis.

### 2.9.3 ISO 27001 Control Objectives

According to ISO 27001:2005 and 2013, 11 clauses define control requirements for ensuring sufficient information security of an organization. The following is the summary of all the 11 clauses of ISO 27001 standard:

- **A.5 Security Policy**: Provides support and direction to the management for information security based on applicable laws and regulations and business requirements.
- **A.6 Organization of Information Security**: For management of information security within and without the organization.

- **A.7 Asset Management**: Attains and preserves proper protection of assets in organization.
- **A.8 Human Resource Security**: Ensures that organizations apply appropriate measures to ensure that all employees are eligible and aware of their roles and responsibilities. It also assures that user access rights are revoked upon termination of employment.
- **A.9 Physical and Environmental Security**: Ensures that systems, buildings, and other supporting infrastructure belonging to an organization are guarded against threats originating from their physical environment.
- **A.10 Communications and Operations**: Ensures proper and secure operation of information processing facilities within the organization.
- **A.11 Access Control**: Manages how users and systems interact with other information assets by making sure that only authorized access is allowed.
- **A.12 System Acquisition, Development, and Maintenance**: Ensures that security of information systems forms an integral part.
- **A.13 Information Security Incident Management**: Ensures timely communication of information security events and vulnerabilities to allow for timely interventions.
- **A.14 Business Continuity Management**: Counteracts interruption of business activities and ensure timely resumption after a disaster
- **A.15 Compliance**: Ensures the organization does not contravene legal, statutory and contractual laws.

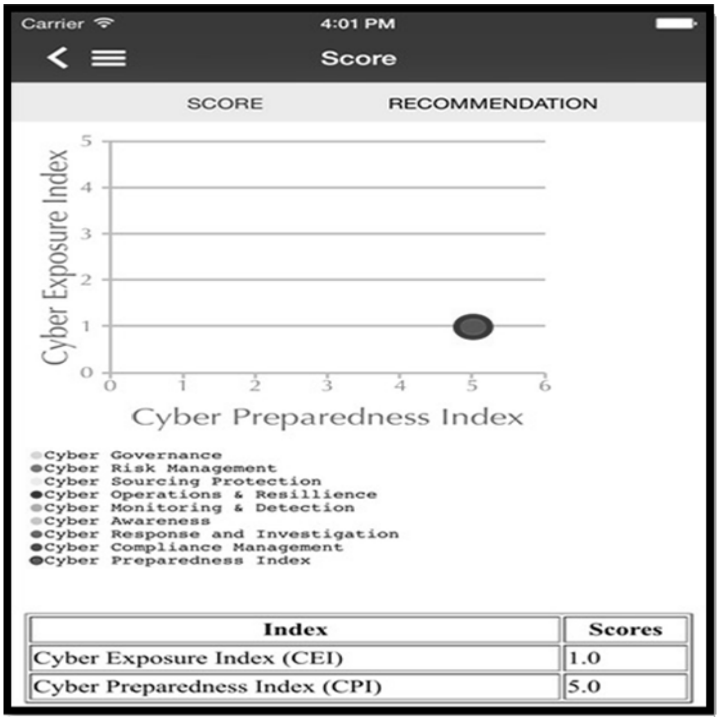
### 2.9.4 Relevant ISO 27001 Control Objectives to SACCOs

According to Brewer & Nash (2010), an organization does not need all controls in their ISMS but can select the controls that are most critical and applicable to their organization based on statement of applicability (SOA). SACCOs in Kenya are financial institutions, which cannot be exempted from the need for ISMS, and therefore it is necessary for these organizations to select appropriate and applicable control objectives for their information security. According to Kigen et al. (2016) survey report on “Kenya Cyber Security” against a checklist of all the 11 ISO/IEC control objectives leads to a narrower list of 6 controls that are considered to be most critical to SACCOs in Kenya. They are; Asset Management, Physical Security, Human

Resource Security, System Security, Access Control, and Compliance In the view of the above, this research used these controls to measure SREI for the SACCOs.

### 2.9.5 Cyber KARE

In 2016, KPMG of India launched a Cyber Security tool called Cyber KARE, which is directed to help senior management in organizations to do self-assessment in order to weigh their echelon of preparedness to fight cyber risks. The model prompts for user input in form of a mobile-based questionnaire with preset radio buttons calculates Cyber Exposure index (CEI) and Cyber Preparedness Index (CPI). The figure below shows the output of Cyber KARE relating the scores of CEI and CPI.



| Index | Scores |
|---|---|
| Cyber Exposure Index (CEI) | 1.0 |
| Cyber Preparedness Index (CPI) | 5.0 |

**Figure 6:** KPMG's Cyber KARE Output

**Source:** (KPMG, 2016)

### 2.9.6 Project Sonar

Rapid 7 have developed a security research project model called Project Sonar which performs internet-wide scanning across diverse services and protocols in order to establish security posture on the internet. The global information about exposure to wide spread threats and vulnerabilities on the internet is made into a report which is availed to the public for further security research (Rapid7, 2017). In 2017 alone, Project Sonar port scanning reported serious security exposures globally uncovering over 15 million open nodes offering telnet and 11.5 million nodes offering direct access to relational database systems (RDBMS). The most exposed nations on the internet, according to the report, are the ones with the largest GDP (Rudis, Beardsley & Harts, 2017).

## 2.10 Research gap

According to the reviewed literature, the researcher noted a gap in the existing models that needed to be filled. Specifically, Rapid 7's Project Sonar focused on the internet against preset protocols and services while KPMG's cyber KARE focused only on senior management of the organizations. Although the two models were used to compute exposure indices, none of ISO 27001 and ISO 27002 standards which are the core of information security, was addressed by the two models. Policy enforcement agencies, regulatory authorities, top management, and any other stakeholders need to have a view of the Security Exposure Index (SREI) based on ISO 27001 best practices as benchmark framework. This research study therefore aimed at filling the gap by designing SREI model with a more comprehensive approach that incorporates six cardinal elements of ISO 27001, namely; asset management, physical security, access control, communication and operations management, system security and human resources security.

## 2.11 Conceptual Framework

In this section, the conceptual framework that guided the research has been presented in two stages; Stage one showed the Conceptual framework for derivation of the formula for computing Security Exposure index, and Stage 2 shows the Conceptual framework for implementation of prototype. Figure 8 below shows the conceptual framework that was used to derive the Security exposure index formula.

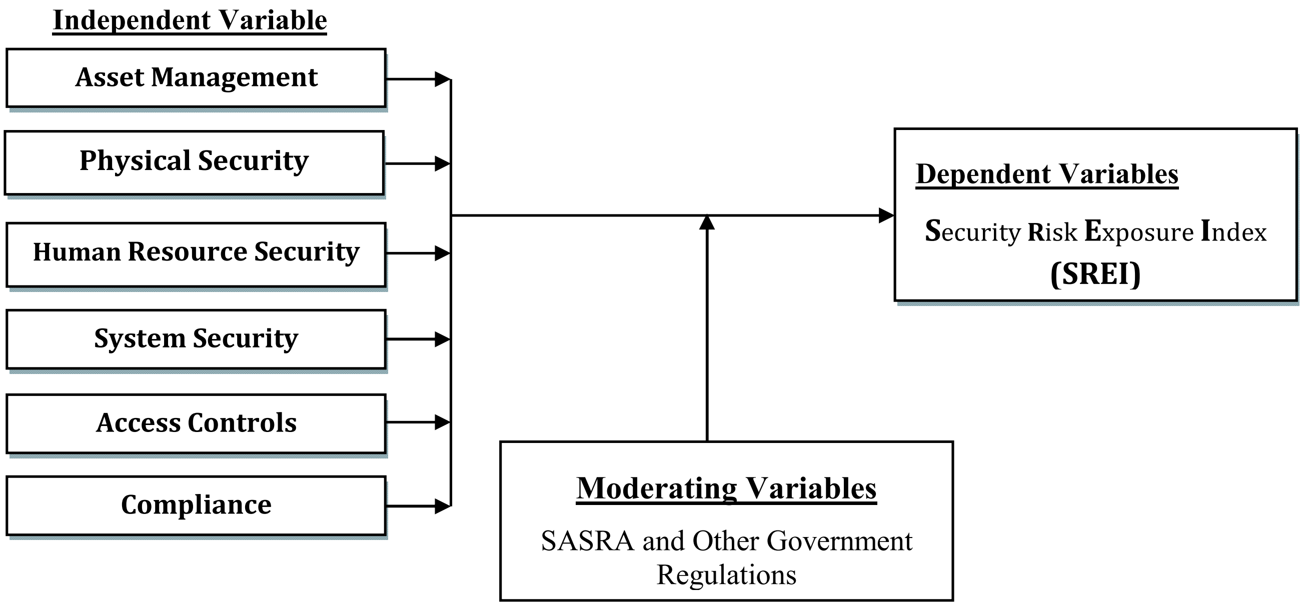


**Figure 7: Conceptual framework for derivation of formula**
**Source: (Researcher, 2017)**

As shown in figure 8, six independent variables selected from 11 clauses of ISO 27001 benchmark standard affects SREI. They are; Asset Management, Physical Security, Human Resource Security, System Security, Access Control, and Compliance. The moderating variables are; SACCO Societies Regulatory Authority (SASRA) and other government regulations. As an advancement of stage one conceptual framework, SREI will be computed as a function of Asset Management, Physical Security, Human Resource Security, System Security, Access Control, and Compliance as shown in the expression below.

*__SREI__=ƒ (__A__sset Management, __P__hysical Security__, H__uman Resource __S__ecurity, __S__ystem Security, __A__ccess Control, __C__ompliance)*

Where,

**Assets Management** is about the position and commitment of the SACCO to assuring proper protection of valuable assets, which include, but not limited to, software, hardware, data, and people.

**Physical Security** is about the position and commitment of the SACCO to preventing illegal physical access, damage, and intrusion to the SACCO's location and information. It involves securing areas with physical security perimeters and entry controls, and securing equipment.

**Human Resource security** is about the SACCO's position and commitment to ensuring that the risk of hiring or contracting the wrong people is mitigated before, during and after change or termination of employment for all contractors, employees, and other third party users.

**System Security** is about the measures put in place by the SACCOs to make sure that security forms the integral part during purchase, development, and maintenance of information application as well as other software.

**Access Controls** is about the the SACCO's commitment to implement physical and logical controls to limit the right of entry to information and information systems

**Compliance** is about the position and commitment by SACCOs to ensuring that they do not violate any civil or criminal law, as well as any contractual, statutory, or regulatory obligations, and any other security needs.

Figure 9 below shows Conceptual framework Stage two which is basically a demonstration of how the prototype implementation was done.

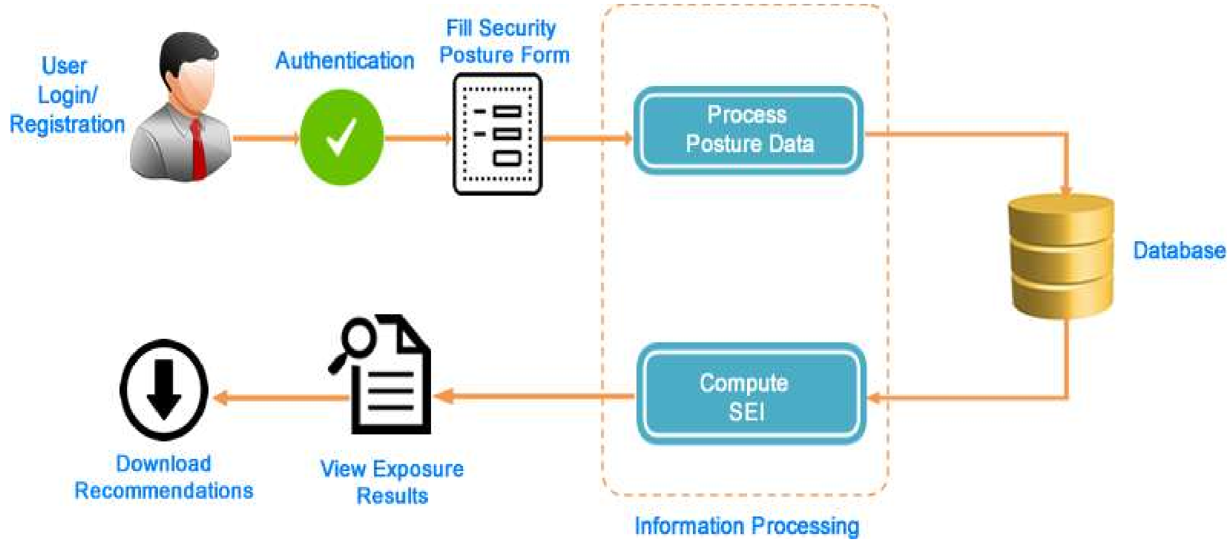


**Figure 8: Conceptual Framework for implementation of prototype**
**Source: (Researcher, 2017)**

The prototype had the following modules; User Registration module, User login and authentication module, which will limit access to, only authorized users. Risk assessment module (digital questionnaire) that prompts the users to feed in posture information to the best of their knowledge. Record management module that stores user information and assessment scores, and information processing module to compute SREI from the stored weights and security posture information provided by the users. In addition, the prototype had a module to display SREI information and provide a mechanism for downloading SREI scores and recommendations.

# CHAPTER THREE
# RESEARCH METHODOLOGY

## 3.1 Introduction

This chapter discusses the research paradigms and research designs and how they were employed in the research. The target population, sample, sample size, sampling technique data collection and analysis are also discussed. It is also in this section that the development, the implementation and the evaluation of the model is discussed. Finally, this chapter outlines the ethical considerations that guided the study.

## 3.2 Research Design

A research design is a comprehensive outline of how a research is to be conducted and involves description of such considerations as data collection methods, types of data collection instruments, how the instruments are used and the way in which the collected data is analyzed (Business dictionary, 2012). In view of the above, this research employed a descriptive survey research design to collect quantitative data. Additionally, this study adopted two research paradigms; scientific paradigm and design science paradigm. The scientific paradigm on one hand was significant for collecting relevant data that was necessary for developing appropriate weights for different security variables. The design science paradigm on the other hand was applicable during implementation of the model.

## 3.3 Location of the Study

This study was carried out in Nakuru East Sub County in Kenya.

## 3.4 Population

This research targeted the SACCOs that were licensed by SASRA as deposit taking within Nakuru. This population was relevant to this study because the target SACCOs had ICT infrastructure and systems in place, which was a pre-requisite for the issuance of licenses.

## 3.5 Sampling Procedure and Sample Size

### 3.5.1 Sampling Procedure

Pre-visit was done to all the eleven deposit-taking SACCOs licensed by SASRA to operate within Nakuru East Sub-county of Nakuru County. The aim was to establish whether they had well established IT infrastructure according to SASRA guidelines, which was also required. A purposive sampling technique for the respondents was used to target those employees who were considered to take the biggest responsibility in matter of security within the SACCOs. These included; the Branch Manager, the ICT manager, the system administrator, the database administrator and the operations Manager. The selected SACCOs also had a well representative spread based on major customer types, namely; Teachers, Farmers, workers, community, and business-based SACCOs.

### 3.5.2 Sample Size

Based on the above sampling technique, the total number of respondents considered for the study was 55. This comprised of five respondents per targeted SACCO who were; the Branch Manager, the ICT manager, the system administrator, the database administrator and the operations Manager.

## 3.6 Data Collection and Analysis Methods

Both primary and secondary data were used in the study. Primary data was collected with structured questionnaires, which were administered, on a drop-and-pick method. The researcher obtained secondary data from the publications of the target SACCOs, security policies, and regulatory authorities. The study used descriptive method to analyze results. These approaches were appropriate because the researcher sought to reprocess hard-to-comprehend security matters into smaller understandable accounts.

## 3.7 Model Design and Implementation

### 3.7.1 Model Design

The Security Risk Exposure Index (SREI) was expected to take a linear form as a function of weight and security variable scores. Therefore, the expected linear equation for the implementation of the model as a mathematical formula would be in the form demonstrated in equation 3 below;

$SREI=W_1V_1+ W_2V_2+ W_3V_3+ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots. + W_nV_n$

**Equation 3: Model Equation**

Where;

$W_1, W_2, W_3 \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots W_n$respectively are different weights that were to be determined from a cross-section of the multiple case results discussed in the study.

While;

$V_1, V_2, V_3 \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots. V_n$ respectively are security variables associated with security risk exposure for which in the case of this study are the sub-components of asset security, physical security, access controls, system security, human resource security, and Compliance. Computation of SREI sought to manage these parameters. Different weights were to be assigned based on the analyzed data collected from the focus SACCOs about present posture of asset security, physical security, human resource security, system security, access controls, and Compliance. On the overall, the model was to compute SREI by comparing SACCO's security posture against thresholds ofISO 27001 best practices. The scores below the threshold were supposed to place the SACCO's security status as wanting. Cases below the threshold values were to trigger actions alerts, for instance, pinpointing security control gaps that need to be filled, and disciplinary action by the regulating authorities.

### 3.7.2 Model Implementation

To implement the model, a rapid prototype was to be designed as a proof of concept. By definition, a *prototype* is a model of something that is to be further developed (Chua *et al.*, 2003). The prototype was to help create preliminary model of the idea and allows for quick testing and evaluation (Mozilla, n.d.). The model was to be in the form of a working web-based application to proof the feasibility of an all-inclusive and final application for managing exposure in financial institutions and other organizations within and beyond Kenya. Figure 10 below shows the rapid prototyping model according to Sabale and Dani (2012)

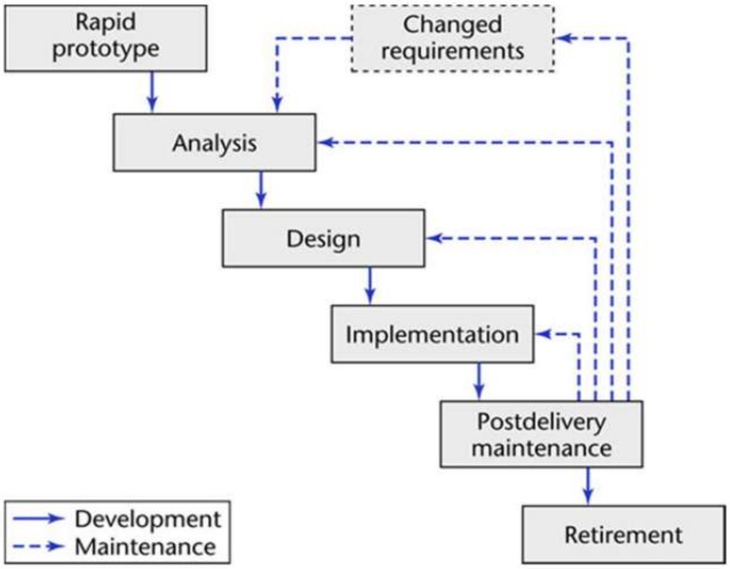


**Figure 9:** Rapid Prototype Model

Source: (Sabale & Dani, 2012)

### 3.7.3 Prototype Evaluation

According to Ryan (2013), testing a prototype allows a concept designs to be evaluated fully, which is sometimes referred to as proof of concept. Put differently, evaluation, simply ascertains that the product will work as expected, or that refinements are needed in order for it to work as expected. In this research, the prototype was to be evaluated using IT-Systems-as-such Goal-based evaluation approach, which is an evaluation approach for determining the extent to which the prototype was achieving the overall preset objectives (Youker, 2014). IT-systems as such evaluation does not involve the users but rather an evaluator and the IT-system involved. The outcome of the evaluation is based on how the evaluator understands the organization and how the system will support it (Cronholm, 2004).

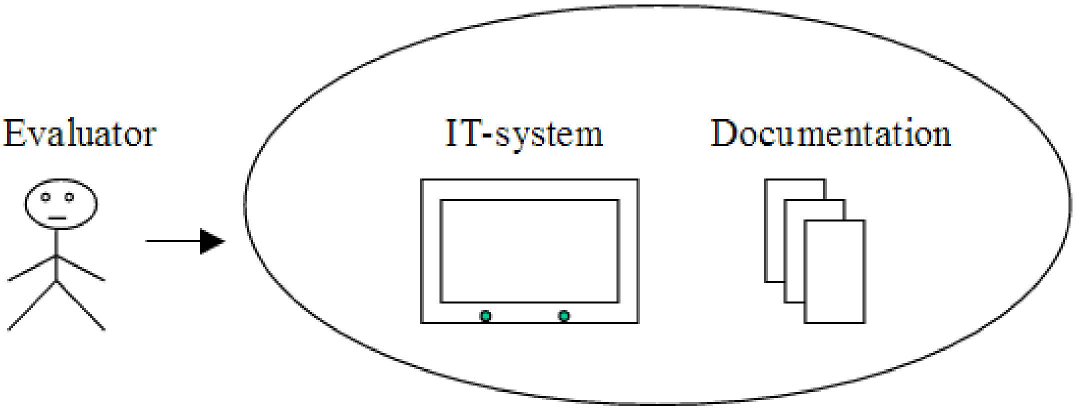


**Figure 10:** IT-Systems as Such goal-based evaluation

**Source**: (Cronholm, 2014)

The prototype evaluation was to focus on evaluating user registration and authentication module for controlling access to the system, use risk assessment module for capturing posture information from the user, Record management module for systematic creation, storage, retrieval and use posture information  and security exposure processing module for computing security exposure factor and comparing it with set exposure thresholds.

### 3.8 Ethical Considerations

The researcher sought to assure the respondents that the study was to be used for academic purposes only and no other purposes. Participation of the respondents was to be on voluntary basis and the respondents could pull out or beg off at any point during the research time. Respondents were not to be coerced into participating in the study but rather were to have prior adequate information about the study from which they could choose to take part or not. Respondents were to be assured that their privacy and confidentiality of their information was to be protected by strict ethical standards of anonymity.

# CHAPTER FOUR
# RESULTS AND DISCUSSION

## 4.1. Introduction

The chapter presents the respondent's basic information, and descriptive findings as per study objectives.

## 4.2. Response Rate

During data collection, 55 respondents were sampled through census method and issued with questionnaires, which duly filled and collected. It was noted that 50 of the questionnaires were returned which translated to a response rate of 91%. The collected questionnaires were therefore used for the study because they were considered enough for providing adequate data.

## 4.3. Respondents basic information

### 4.3.1. Position held in the SACCO

Respondents were asked to provide information on their position in the SACCO as to whether they were full-time employees or part-time employees. The respondents' position in the SACCO is presented in Table 2 below.

**Table 4.1: Position held in the SACCO**

| Variable | | Freq | Percentage (%) |
|---|---|---|---|
| Valid | Full time employee | 30 | 60.0 |
| | Part time employee | 20 | 40.0 |
| | **Total** | **50** | **100.0** |

The responses shown in Table 2 above showed that a majority of respondents constituted full time employees (60% of the population) whereas only 40% of the total population constituted part-time employees.

### 4.3.2. Membership of the SACCO

The respondents were requested to provide information on the major constituents of their membership within the SACCO. The responses are presented in Table 3 below.

**Table 4.2: Membership of the SACCO**

| Variable | | Freq | Percentage (%) |
|---|---|---|---|
| | Teachers | 30 | 60.0 |
| | Farmers | 3 | 6.0 |
| Valid | Workers | 10 | 20.0 |
| | Doctors | 2 | 4.0 |
| | Business | 5 | 10.0 |
| | **Total** | **50** | **100.0** |

It was evident from the analyzed data that teachers constituted a larger catchment for the SACCO in Nakuru with 60%. The responses further depicted that workers constituted (20%), business (10%), farmers (6%) and doctors (4%).

### 4.4 Descriptive Findings

This section presents descriptive statistics regarding the variables under study. Frequencies and percentages were used to analyze the data. The finding is as presented in the following sections.

### 4.4.1 Critical Nature of ISO 27001 Security Risk Factors in SACCOs

In order to attain objective one, the respondents were asked to give their opinion on the criticality of the eleven ISO 27001 security factors. The responses are presented in Table 4 below.

**Table 4.3: Critical Nature of ISO 27001 Security Risk Factors in SACCOs**

| Ratings | NVC | NC | N | C | VC |
|---|---|---|---|---|---|
| **Statement** | **Freq(%)** | **Freq(%)** | **Freq(%)** | **Freq(%)** | **Freq(%)** |
| Security Policy | 20(40.0) | 30(60.0) | 0(0.0) | 0(0.0) | 0(0.0) |
| Physical and Environmental Security | 0(0.0) | 0(0.0) | 0(0.0) | 15(30.0) | 35(70) |
| Human Resource Security | 0(0.0) | 5(10.0) | 3(6.0) | 15(30) | 27(54) |
| Asset Management | 0(0.0) | 0(0.0) | 0(0.0) | 8(16.0) | 42(84.0) |
| Communication Management & Operations Management | 4(8.0) | 40(80.0) | 6(12.0) | 0(0.0) | 0(0.0) |
| Organization of Information Security | 18(36.0) | 32(64.0) | 0(0.0) | 0(0.0) | 0(0.0) |
| System Security | 0(0.0) | 3(6.0) | 4(8.0) | 18(36.0) | 25(50.0) |
| Access Control | 1(2.0) | 6(12.0) | 1(2.0) | 19(38.0) | 23(46.0) |
| Information Security Incident Management | 16(32.0) | 30(60.0) | 4(8.0) | 0(0.0) | 0(0.0) |
| Business Continuity Management | 16(32.0) | 34(68.0) | 0(0.0) | 0(0.0) | 0(0.0) |
| Compliance | 0(0.0) | 5(10.0) | 5(10.0) | 0(0.0) | 40(80.0) |

**Key**: NVC=Not Very Critical, NC= Not Critical, N=Neutral, C=Critical, VC=Very Critical, freq=frequency, and%=Percentages

Source: Research Data (2017)

As it can be seen from the analyzed data presented in Table 4 above, the security risk factors that were considered to be very critical or critical (VC%, C%) to SACCO included; Physical and Environmental Security (70%, 30%). Human Resource Security (54%,30%). Asset security and management (84%, 16%). System Security (50%, 36%). Access Control(46%,38%), and Compliance(80%,0%).However, the respondents consider the following risk factors to be not very critical or not critical (NVC%,NC %); Security policy(60%,40%); communications & Operations Management (8%,80%); Organization of Information Security (36%,64%); Business Continuity Management(32%,68%); and Information Security Incident Management (32%,60%) were considered as not critical.

### 4.4.2 Asset Security and Management

An assessment was done regarding asset security and management as a critical security risk factor where the respondents were required to give their responses on whether they strongly disagree, disagree, were neutral, agree, or strongly agree to the statements about Asset security and management within their SACCO. The findings are presented in Table 5 below.

**Table 4.4: Asset Security and Management**

| **Statement** | **SD** | **D** | **N** | **A** | **SA** |
|---|---|---|---|---|---|
| There is an up-to-date inventory of all assets in form of information and information processing facilities. | 18<br>36.0% | 32<br>64.0% | 0<br>0.0% | 0<br>0.0% | 0<br>0.0% |
| There are clearly defined owners for all information assets. Owners know their responsibilities. | 1<br>2.0% | 32<br>64% | 8<br>16.0% | 9<br>18.0% | 0<br>0.0% |
| Acceptable-use-policy applies for each type / class of information asset and all users are conscious of it before they use. | 11<br>22.0% | 33<br>66.0% | 0<br>0.0% | 6<br>12.0% | 0<br>0.0% |
| There is a formal process for ensuring that all employees and external users return institution’s assets upon end of contract, agreement, or employment. | 9<br>18.0% | 41<br>88.0% | 0<br>0.0% | 0<br>0.0% | 0<br>0.0% |
| There is a formal process through which all information is appropriately categorized and all users of information assets understand it. | 16<br>32.0% | 30<br>60.0% | 4<br>8.0% | 0<br>0.0% | 0<br>0.0% |
| There is a policy governing use, transport, and disposal of removable media and all employees are aware of it. | 20<br>40.0% | 30<br>60.0% | 0<br>0.0% | 0<br>0.0% | 0<br>0.0% |

**Key**: SD=Strongly Disagree; D=Disagree; N=Neutral; A=Agree; SA=Strongly Agree; Freq=Frequency, and%=Percentages

**Source**: Research Data (2017)

Regarding asset security and management as a critical security risk factor, the finding indicated that respondents generally disagreed that there was an up-to-date and accurate record of all assets in form of information processing facilities as well as information with 36% strongly disagreeing and 64% disagreeing. Whether there was a formal procedure for proper classification of information for which the users understood, the responses showed that the majority of the respondents (64%) did not agree. Whether there was a well-communicated acceptable use policy for each class of assets, the responses depicted that 22% of respondents strongly disagreed. 66% disagreed and 12% agreed. Further, respondents did not agree to the fact that there was a formal process for returning organizational assets upon termination of employees (88%) and that there is no well defined and enforced policy governing use, transport and disposal of removable media that all employees were aware of (60%). This finding therefore validates the fact that asset Security and Management is critical factor in analyzing security Risk Exposure index of a firm.

### 4.4.3. Physical and Environmental Security

An investigation was done vis-à-vis physical and environmental security as a critical security risk factor where respondents were required to provide information in agreement or otherwise of the statements associated with physical and environmental security as a critical factor of security. The findings are presented in Table 6 below.

**Table 4.5: Physical and Environmental Security**

| Statement | SD | D | N | A | SA |
|---|---|---|---|---|---|
| The organization has installed a designated | 0 | 0 | 17 | 33 | 0 |
| security perimeter. | 0.0% | 0.0% | 34.0% | 66.0% | 0.0% |
| Risks from unauthorized access / passers-by | 0 | 10 | 7 | 33 | 0 |
| considered when siting equipment | 0.0% | 20.0% | 14.0% | 66.0% | 0.0% |
| There is a UPS system or backup generator in | 0 | 44 | 0 | 6 | 0 |
| place that is tested within an appropriate timescale | 0.0% | 88.0% | 0.0% | 12.0% | 0.0% |
| The location of power and telecommunications | 8 | 42 | 0 | 0 | 0 |
| cables protect from interference, interception or damage. | 16.0% | 84.0% | 0.0% | 0.0% | 0.0% |
| There is a well-enforced and well-communicated | 0 | 45 | 5 | 0 | 0 |
| process controlling how assets are removed from site and spot checks are carried out. | 0.0% | 90.0% | 10.0% | 0.0% | 0.0% |
| Policies and technical controls apply in securing | 11 | 30 | 0 | 0 | 9 |
| equipment that are inadvertently left unattended. | 22.0% | 60.0% | 0.0% | 0.0% | 18.0% |
| A clear desk and/or clear screen policy are well | 0 | 31 | 5 | 14 | 0 |
| enforced in the organization | 0.0% | 62.0% | 10.0% | 28.0% | 0.0% |

Key:SD=Strongly Disagree; D=Disagree; N=Neutral; A=Agree; SA=StronglyAgree and%=Percentages

**Source**: Research Data (2017)

The results of the analyzed data revealed that 66% of the respondents agreed that the organization had installed a designated security perimeter. In similar manner, respondents agreed that risks of access by passers-by and other unauthorized persons were being considered at the time of siting equipment (66%). A smaller number of respondents noted that there was a UPS system or backup generator in place that is tested within an appropriate timescale (12%) with 88% generally disagreeing. However, 90% of the respondents disagreed to the statement that there was a well-enforced and well communicated process of controlling how assets are removed from site and spot checks are carried out. Further, 82% or the responses showed that the respondents disagreed that the location of power and telecommunications cables were protected from damage, interference, or interception. 82 percent disagreed that there were technical controls and policies in place to secure equipment that has been inadvertently left unattended, while 62% disagreed to the statement that there was a clear desk or clear screen policy that was well enforced. These findings therefore confirm that security risk exposure related to physical and environmental security was key and require more focus by SACCOs.

### 4.4.4. System Security

An inquiry was done to determine how respondents would agree to the statements related to system security as a critical security risk factor. The findings are presented in Table 7 below.

**Table 4.6: System Security**

| Statement | SD | D | N | A | SA |
|---|---|---|---|---|---|
| The SACCO develops software or systems in-house and there are policies mandating the implementation and assessment of security controls. | 9<br>18.0% | 33<br>66.0% | 8<br>16.0% | 0<br>0.0% | 0<br>0.0% |
| The SACCO specifies information security requirements during introduction, enhancement or upgrade of systems. | 0<br>0.0% | 20<br>40.0% | 20<br>40.0% | 10<br>20.0 % | 0<br>0.0% |
| The SACCO applications that send information over public networks properly shield the information against fraud, contract dispute, unauthorized disclosure, and unauthorized modification. | 5<br>10.0% | 33<br>66.0% | 12<br>24.0% | 0<br>0.0% | 0<br>0.0% |
| There are controls in place for preventing information misrouting, incomplete transmission, unauthorized message alteration, unauthorized disclosure, replay attacks, or unauthorized message duplication. | 7<br>14.0% | 35<br>70.0% | 7<br>14.0% | 1<br>2.0% | 0<br>0.0% |
| There are policies in place that mandate how and when software packages can be changed or modified | 11<br>22.0% | 35<br>70.0% | 4<br>8.0% | 0<br>0.0% | 0<br>0.0% |
| Where software is developed in-house, proper utilization of secure development environment for all | 0<br>0.0% | 19<br>38.0% | 31<br>62.0% | 0<br>0.0% | 0<br>0.0% |

| | | | | | |
|---|---|---|---|---|---|
| projects apply during the system development lifecycle | | | | | |
| There are requirements that externally developed code must be subjected to a security review and test before deployment | 9<br>18.0% | 37<br>74.0% | 0<br>0.0% | 4<br>8.0% | 0<br>0.0% |

**Key:** SD=Strongly Disagree; D=Disagree; N=Neutral; A=Agree; SA=Strongly Agree and%=Percentages

**Source**: Research Data (2017)

As presented in Table 7 above, the findings showed clearly that respondents agreed that the SACCO specify information security requirements during introduction, enhancement, or upgrade of systems (20%). It was observed that 62% of the respondents were undecided whether proper utilization of secure development environment applied to all projects during the system development lifecycle. Conversely, it was observed that a majority disagreed that the SACCO develop software or systems in-house and there are policies mandating the implementation and assessment of security controls (84%). Further, 76% of the respondents disagreed that the SACCO applications that send information over public networks properly could shield the information against fraud, contract dispute, unauthorized disclosure, and unauthorized modification. It was observed that a greater part of the respondents similarly disagreed that there are policies in place that mandate how and when software packages can be changed or modified. There are controls in place for preventing information misrouting, incomplete transmission, unauthorized message alteration, unauthorized disclosure, replay attacks or unauthorized message duplication and that there are requirements that externally developed code must be subjected to a security review and test before deployment with 84% and 82% respectively. These finding suggest that system security is a key component in analysis of security risk exposure index, which will be the focus of this study.

### 4.4.5. Human Resource Security

The study further sought to investigate how respondents would agree to the statements related to Human Resource Security as a critical security risk factor. The findings are presented in Table 8 below.

**Table 4.7: Human Resource Security**

| Statement | SD | D | N | A | SA |
|---|---|---|---|---|---|
| Background verification checks apply to all employment candidates and are approved by appropriate management authority. | 0<br>0.0% | 14<br>28.0% | 5<br>10.0% | 31<br>62.0% | 0<br>0.0% |
| All employees and contractors must sign confidentiality and nondisclosure agreements | 0<br>0.0% | 0<br>0.0% | 20<br>40.0% | 30<br>60.0% | 0<br>0.0% |
| Managers engage in driving security within the SACCO and encourage all contractors and employees to apply security according to laid down policies and procedures. | 0<br>0.0% | 10<br>20.0% | 0<br>0.0% | 40<br>80.0% | 0<br>0.0% |
| All employees and contractors undergo security awareness training regularly that is appropriate to their roles and function within the SACCO. | 8<br>16.0% | 38<br>76.0% | 0<br>0.0% | 4<br>8.0% | 0<br>0.0% |
| There is an official disciplinary process through which the organization acts upon employees who breach information security. All employees are aware of the process. | 0<br>0.0% | 0<br>0.0% | 5<br>10.0% | 45<br>90.0% | 0<br>0.0% |
| There is a documented process for changing employment duties or terminating employment that is communicated to the employees and/or contractors | 0<br>0.0% | 20<br>40.0% | 0<br>0.0% | 30<br>60.0% | 0<br>0.0% |

**Key**: SD=Strongly Disagree; D=Disagree; N=Neutral; A=Agree; SA=Strongly Agree and%=Percentages

**Source**: Research Data (2017)

As shown in Table 8 above, the finding indicated that respondents agreed that there are background verification checks, which applied to all employment candidates and was approved by appropriate management authority (62%). Others aver that there is an official disciplinary process, known by over 90%, through which the organization acts upon employees who breach information security. In a similar manner, 60% agreed that all employees and contractors must sign confidentiality and nondisclosure agreements. It was further perceived that 80% of respondents agreed that managers were engaged in driving security within the SACCO and encourages all contractors and employees to apply security according to laid down policies and procedures. While 60% agreed that, there was a documented process for changing employment duties or terminating employment that is communicated to the employees and/or contractors. In contrast, 76% of the respondents disagreed that all employees and contractors undergo security awareness training regularly that is appropriate to their roles and functions within the SACCO. These revelations posit that human resource development has a direct link on organizational security management, which the present study seeks to lay an emphasis on.

### 4.4.6. Access Controls

A study was done and respondents were asked to provide information to agree or otherwise to the statements related to Access Controls as a critical security risk factor. The findings are presented in Table 9 below.

**Table 4.8: Access Controls**

| Statement | SD | D | N | A | SA |
|---|---|---|---|---|---|
| There is a well-documented and widely communicated access control policy in the organization. | 0<br>0.0% | 16<br>32.0% | 8<br>16.0% | 26<br>52.0% | 0<br>0.0% |
| Controls exist for ensuring that users can only access network resources necessary for their duties. | 0<br>0.0% | 12<br>24.0% | 0<br>0.0% | 38<br>76.0% | 0<br>0.0% |
| The SACCO has a formal user access registration process and a formal access assignment process to assign access rights for all users. | 0<br>0.0% | 17<br>34.0% | 0<br>0.0% | 33<br>66.0% | 0<br>0.0% |
| Formal management processes and policies are in place for controlling the allocation of secret authentication. | 0<br>0.0% | 20<br>40.0% | 27<br>54.0% | 3<br>6.0% | 0<br>0.0% |
| Processes exist for ensuring that user access rights are revoked upon termination of contractor employment, or adjusted when their roles change. | 0<br>0.0% | 5<br>10.0% | 1<br>2.0% | 44<br>88.0% | 0<br>0.0% |
| Strict access control policy applies to restrict access to information and application system functions. | 0<br>0.0% | 23<br>46.0% | 3<br>6.0% | 24<br>48.0% | 0<br>0.0% |
| Password systems are interactive and enforce complex passwords requirements | 19<br>38.0% | 26<br>52.0% | 5<br>10.0% | 0<br>0.0% | 0<br>0.0% |

**Key**: SD=Strongly Disagree; D=Disagree; N=Neutral; A=Agree; SA=Strongly Agree and%=Percentages

**Source**: Research Data (2017)

The results of the analyzed data as posted in Table 9 indicated that 88% of the respondents agreed that processes existed for ensuring that user access rights are revoked upon termination of contract or employment, or adjusted when their roles changes. This is a good measure in ensuring that access to critical information is safeguarded by an organization. This view was supported by 76% and 52% of the respondents who affirmed that controls existed for ensuring that users can access only the network resources necessary for their duties, and that there was a documented access control policy that was communicated appropriately respectively. In addition, 66% aver that the SACCO had a formal user access registration process and a formal user access assignment process to assign access rights to all users. Conversely, 54% of the respondents were undecided as to whether formal management processes and policies were in place for controlling the allocation of secret authentication. It was clear from the findings that respondents disagreed to the statements that password systems were interactive and enforce complex passwords requirements, and that access to application system functions and information were restricted using access control policy with 52% and 46% respectively.

### 4.4.7. Compliance

A study was further carried out where respondents were required to provide information in agreement or otherwise of the statements related to Access Controls as a critical security risk factor. The findings are presented in Table 10 below.

**Table 4.9: Compliance**

| Statement | SD | D | N | A | SA |
|---|---|---|---|---|---|
| Our SACCO has identified and documented all applicable contractual, legislative or regulatory requirements concerning security | 0<br>0.0% | 20<br>40.0% | 30<br>60.0% | 0<br>0.0% | 0<br>0.0% |
| The SACCO maintains a record of all proprietary software products and intellectual property rights and monitor use of unlicensed software | 0<br>0.0% | 26<br>52.0% | 18<br>36.0% | 6<br>12.0% | 0<br>0.0% |
| All the records within the SACCO are protected from loss, destruction, falsification and unauthorized access or release in conformity with contractual, regulatory, legislative and business requirements | 9<br>18.0% | 28<br>56.0% | 10<br>20.0% | 3<br>6.0% | 0<br>0.0% |
| The SACCO protect personal data in strict compliance with relevant legislation | 0<br>0.0% | 0<br>0.0% | 0<br>0.0% | 45<br>90.0% | 5<br>10.0% |
| The SACCO ensures that the implementation of security controls and information security is subject to regular independent reviews | 5<br>10.0% | 0<br>0.0% | 0<br>0.0% | 16<br>32.0% | 29<br>58.0% |
| The SACCO managers do under instruction to-do policy and procedures' compliance reviews within their area of responsibility regularly | 0<br>0.0% | 46<br>92.0% | 0<br>0.0% | 4<br>8.0% | 0<br>0.0% |
| The SACCO conducts technical compliance reviews of information systems regularly | 20<br>40.0% | 30<br>60.0% | 0<br>0.0% | 0<br>0.0% | 0<br>0.0% |

**Key**: SD=Strongly Disagree; D=Disagree; N=Neutral; A=Agree; SA=Strongly Agree and%=Percentages

**Source**: Research Data (2017)

The findings presented in Table 10 above revealed that 52% and 74% of the respondents disagreed that the SACCO maintained a record of all proprietary software, intellectual property rights. Monitors the use of unlicensed software and that all the records within the SACCO were protected from loss, destruction, falsification and unauthorized access or release in conformity with contractual, regulatory, legislative and business requirements. In a similar vein, nearly all the respondents disagreed that the SACCO managers were instructed to carry out compliance reviews with policies and procedures within their area of responsibility regularly and that the SACCO conducted technical compliance reviews of information systems regularly with 92% and 100% respectively. However, all the respondents agreed that the SACCO protected personal data in strict compliance with relevant legislation (100%) and that the SACCO ensured that the implementation of security controls and information security was subject to regular independent reviews (90%). It was observed that respondents were undecided on whether their SACCOs had identified and documented all applicable contractual, legislative, and regulatory requirements related to security (60%)

### 4.5 Derivation of Relevant Weight for SREI Mathematical Model

To obtain Security Risk exposure index (SREI) of an organization, Risk assessment questions were asked where respondents were to answer in a scale of 1 to 5 whereby 1 meant that the respondent was strongly disagreeing to assessment statement while 5 meant that the respondent was strongly agreeing to the assessment statements. In the same tone, the other responses included; Disagree, Neutral and Agree.

The scores of the respondent per assessment question denoted the level of compliance to ISO 27001 standards by the respondent and associated organization, which in this case was referred to as Security maturity factor of the organization (Y). The following linear regression modeling equation was used to compute weights necessary for computing Security maturity factor (Y) and by extension the Security Risk Exposure Index (SREI).

$$\mathbf{Y= W_1V_1 + W_2V_2 \ldots + W_nV_n}$$

Where;

| | | |
|---|---|---|
| Y | = | Security Maturity factor of the organization |
| W | = | Weights |
| V | = | Security Variable (User assessment Score per question) |
| n | = | Number of assessment questions |

Suppose all the assessment questions have constant coefficients, such that $W=W_1=W_2=\ldots W_,$ Then, the weight will be W, whereby;

$$\mathbf{Y = WV_1+WV_2+WV_3+\ldots WV_n.}$$

Since W is common,

$$\mathbf{Y= W(V_1+V_2+V_3+ \dots Vn)}$$

Equation 4: Mathematical Maturity Model

In the case of the this study, there were 40 questions that were used for Security Risk Assessment, in which case, n=40 and the maximum score that the user could have in a scale of 1 to 5 was; 5*40 = 200.

If we put back this to maturity equation 4 above, then;

$$\mathrm{Y} = \frac{\mathrm{V1}}{200} + \frac{\mathrm{V2}}{200} + \frac{\mathrm{V3}}{200} + \dots \frac{\mathrm{V40}}{200}$$

Therefore;

$$\mathrm{Y} = \frac{1}{200}(\mathrm{V1} + \mathrm{V2} + \mathrm{V3} + \dots \mathrm{V40})$$

Hence;

$$\mathrm{W} = \frac{1}{200} = 0.005$$

In the view of the above, the relevant weightfor the SREI model based on 40 Assessment questions was **0.005**;

The value of maturity factor Y could be represented as a percentage factor (Y %) as shown in equation 5 below;

$$\mathrm{Y} = 0.005(\mathrm{V1} + \mathrm{V2} + \mathrm{V3} + \dots \mathrm{V40}) * 100$$

Hence

$$\mathbf{Y = 0.5(V1 + V2 + V3 + \dots V40)\%}$$

Equation 5: Percentage Maturity Factor

### 4.5.1 SREI Mathematical Model

By achieving the weight and the maturity model of the organization, which denotes the level of compliance to the ISO 27001 standard, as shown in equation 5 above, SREI was computed as a level of immaturity or non-compliance to ISO 27001 standard. SREI represented the gap between full compliance to ISO 27001 standard and the actual posture of the organization represented by the maturity score. The equation for computing SREI as a percentage factor was therefore derived as follows;

$$\mathbf{SREI = 100 - Y\%}$$

Since Y% was already derived in equation 5, then by substitution, the complete percentage SREI equation was a shown in equation 6 below;

$$\mathbf{SREI = 100 - \{0.5(V1 + V2 + V3 + \ldots V4\ 0)\}}$$

Equation 6: SREI Mathematical Model

## 4.6 Model Scenarios

The Security Risk exposure Index of an organization was determined by first maturity factor of the organization as shown in equation 5 which represented the compliance level of the organization to ISO 27001 standard. Second computing SREI as shown in equation 6, which represents the organizations deficit score, or gap for it to attain full compliance to ISO 27001 standard. There are therefore three model scenarios, which are explained in sections 4.5.1 to 4.5.3, namely; Best-case scenario, Average case scenario, and Worst-case scenario.

### 4.6.1 Best case scenario

The best-case scenario is achieved when sum of assesses scores for the 40 risk assessment questions is equal to 200.

That is; $\mathbf{V1 + V2 + V3 + \cdots V4\ 0 = 200}$

By substituting back to equation in equation 5,

$\mathbf{Y = 0.5(200) = 100\%}$;

Equation 7: Best case scenario maturity factor

By substituting back to equation 6,

$\mathbf{SREI = 100 - \{0.5(200)\} = 0\%;}$

Equation 8: Best case scenario SREI

Equations 7 and 8 above depicts that the user and their organization are fully compliant to the specific requirements of ISO 27001 standard at Y=100% and that it is Least exposed at SREI = 0%.

### 4.6.2 Average Case scenario

The average case scenario is the middle position whereby the organization is 50% exposed and 50% mature. In a scale of 1 to 5, which was the case in this study, the average case scenario is where the assesse scored an average of 2.5 per question or total score of 100 for the 40 assessment questions, which tends towards a neutral score. This implies that the organization is neutral and can neither be fully compliant to ISO 27001 requirements nor fully exposed. The following equations 9 and 10 presents the maturity and exposure factors for the average case scenarios respectively.

$\mathbf{Y = 0.5(100) = \ 50}\%$ ;

Equation 9: Average case scenario maturity score

$\mathbf{SREI = 100 - \{0.5(100)\}= 50\%}$

Equation 10: Average case scenario SREI

### 4.6.3 Worst Case scenario

The worst-case scenario is the converse of the best-case scenario whereby the assessment scores depict that the user and their organization are least mature in terms of compliance to specific requirements to ISO 27001 standards whereforeY → 0%. This also imply the organization is much exposed with their SREI tending towards 100%; that is, SREI → 100%. When scores in a scale of 1 to 5 are used as was the case in this study, the worst-case scenario is attained when the assessee attains an average of 1 per question or a sum of 40 for all the 40 assessment questions. Therefore, the worst-case scenario values for maturity factor and exposure factor are presented in equations 11 and 12 respectively.

$\mathbf{Y = 0.5(40) = \ 20}\%$ ;

Equation 11: Worst case scenario maturity factor

$\mathbf{SREI = 100 - \{0.5(40)\}= 80\%;}$

Equation 12: Worst case scenario SREI

### 4.6.4 Threshold Scores and assessment scale

According to SREI model, the threshold scores, which are in a scale of 1 to 5, were pegged at 4. This score denotes that the assessee agrees to be compliant to the requirements of ISO 27001 standard. Score 5, which denote that the assessee is in strong agreement with the issue of compliance with ISO 27001 standard requirements. This meant that the assessee's average score per assessment question was at a mature 5 and therefore the least exposure factor. However, average scores of 1,2 and 3 which are below the threshold score (4) means that the user's exposure index is increasingly tending towards 80% which is considered to be highly risky case for the organization. These scenarios therefore call for action by the organization to minimize the risk. Recommendations for best practices are therefore pegged on these threshold scores.

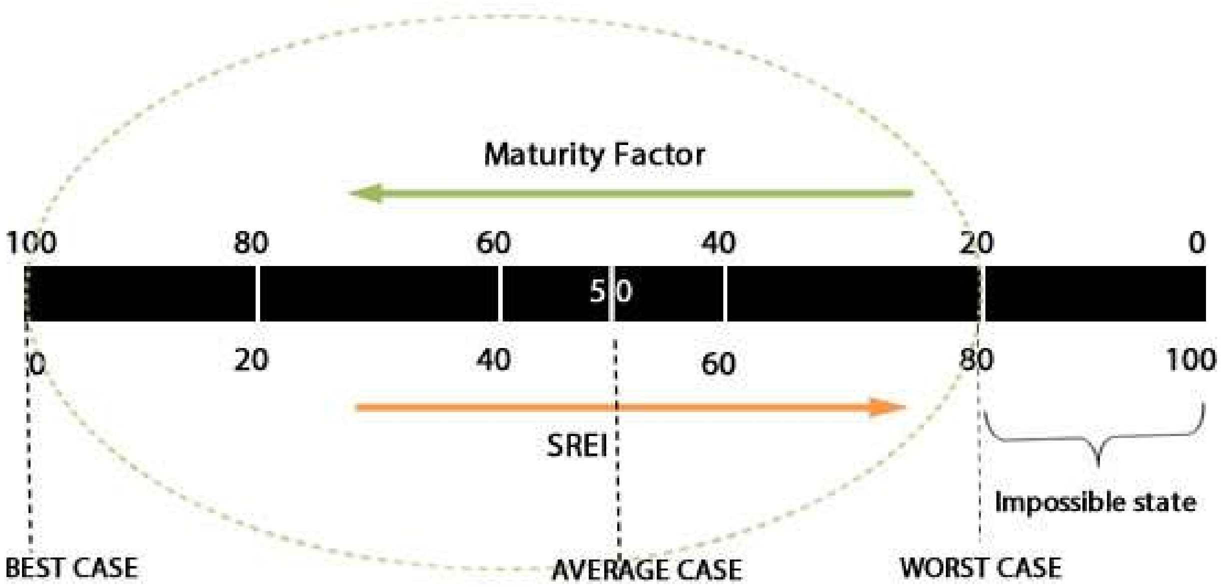


**Figure 11: Assessment Scale**

**Source: Researcher (2017)**

As presented in the equations 11 and 12 above, the worst-case scenario is represented by 20% maturity and 80% exposure factors respectively. The 0% maturity and 100 exposure factors cannot be computed from the model because the model computation for these factors is pegged on a scale of 1 to 5, which yields the said results. This is called the impossible state as shown in the figure 12.

# CHAPTER FIVE

## MODEL IMPLEMENTATION

### 5.1 Introduction

This chapter attempts to answer research question three by providing a detailed discussion of the entire process that was followed in the implementation of security risk exposure index (SREI) model as a web-based prototype.

### 5.2 SREI System Design

This section presents SREI Platform overview starting with system objectives, system functional overview, participants in the system, Processes to achieve SREI system functionality, system architecture and system interface. The design overview is further decomposed into 6 sections; namely, section 5.2.1 to section 5.2.6 that describes the process that was followed in the development of the model.

### 5.2.1 System Objectives

The main objective of this study was to design a web-based platform that would enable Savings and credit cooperative societies and possibly other organizations to perform their independent assessment to determine their Security Risk exposure Index (SREI). SREI informs the organizations about how much they are exposed to security threats based on ISO 27001 ISMS requirements. The platform also helps Sacco Societies Regulating Authority (SASRA) and other government agencies to monitor the SACCOs for compliance with security risk management standard requirements.

### 5.2.2 System Functional Overview

In an attempt to help organizations perform independent assessment to ascertain their level of exposure to security threats, SREI platform was developed using PHP as server side scripting language, Mysql as a database engine, CSS3 for styling and JQuery for interactive functions. Security was enforced in the web-based model to ensure that users were authenticated before performing security risk assessment, viewing their assessment information, or accessing any other system functionality. All users were required to register by providing their names,

names of their organizations, their usernames, password, and confirmation of their passwords. The platform keeps users’ assessment records by associating with current time stamps.

### 5.2.3 System Participants

The SREI platform has a number of participants, who include; System users, System Administrators, Domain name registrar, and web hosting service provider.

a) **Users:** Users of SREI system are those who login successfully and are able to carry out assessment tasks within the SREI platform, for instance, checking their previous assessment history, performing fresh assessment, checking their previous and current scores and downloading their current and/or previous assessment recommendations.

b) **Administrators:** users with elevated privileges within the SREI platform are called Administrators. This is reserved for regulating authorities, system administrators, and other government agencies that may be players in management of security risks within organizations. Unlike the other system users, administrators are able to view the overall trends of exposure indices from user assessments over time, update assessment checklists when ISO 27001 checklist change.

c) **Domain registrars:** A Domain name registrar is a commercial entity or an organization that manages the reservation of internet domain names. In this case, they are responsible for registration and reservation of the domain name for the SREI system on the internet.

d) **Web host:** Also referred to as web hosting service providers, they ensure that there is guaranteed availability of the system online by providing hosting space on their servers as well as services and technologies required for the WebPages to be displayed on the Internet. The web server allows for the two-way communication between users and the SREI system setting up, maintaining, and closing sessions.

### 5.2.4 Processes to Complete SREI System functionality

The SREI system was achieved though rapid prototyping that was discussed in section 3.7. The following processes were followed to guide the development.

a) **Requirements Gathering Process:** The requirements for the SREI System were gathered from the security posture portrayed in SACCOs and the climbing threat landscape as depicted in chapter 2.

b) **Quick design Process:** A quick conceptual design of system database and modules was done using flow diagrams as summarily shown in figure 9. The quick design of different modules is portrayed in figure 13below.

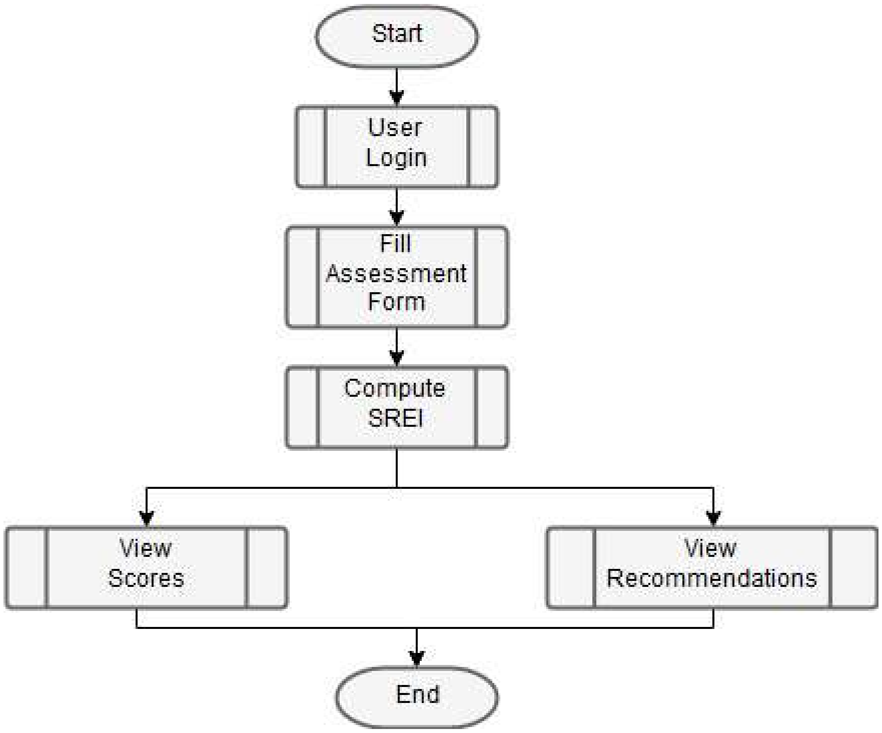


**Figure 12: Web-based SREI System Flowchart**

**Source: Researcher (2017)**

c) **Prototype Design Process:** PHP server side scripting language was used to develop the prototype, JQuery was used for interactive functionality of the system, CSS3 was used for styling the interface, and MySQL as the database engine.

d) **Evaluation Process:** The prototype was evaluated using IT-Systems as Such goal-based evaluation presented in section 3.7 against gathered system objectives. The same approach guided ongoing refinement process.

e) **Coding and testing Processes:** The code was refined upon the achievement of satisfactory requirements. The final version of the system was deployed and the real users were allowed to register and test all system functionalities. Feedback informed some further development and refinement of both the model and system is ongoing as feedback is received from the users from this stage.

f) **Deployment Process:** A complete prototype files and database were deployed online

### 5.2.5 SREI System Architecture

SREI system is an assembly of independent components, herein, referred to as modules. The hub of the architecture comprises of the following key components;

a) **User authentication module:** This module is responsible for ensuring that only registered users who have express permissions to access system functionality are allowed to do so and others denied access.

b) **User Registration Module:** This module is an entry point to the SREI system that allows the user to register by providing compulsory information such as user's full name, organization, username, email, and password. Only registered users are allowed to access system functionality.

c) **Password management Module:** This module handles password complexity requirements and password verification. It also allows encryption of user passwords on database level using MD5 cryptographic hash function.

d) **User Session Handling module:** This module handles user sessions by setting user sessions when they successfully login, track all the user activities when the session is on, and unset (destroy) the session when the user logs out of the system

e) **Risk Assessment module:** This module retrieves the questions from the database and presents them in likert scale layout where the user can read the questions, check the most appropriate option for each question depending on their organization's posture, and submit duly filled assessment form.

f) **Results module:** This module presents results of submitted assessments to the user in an interactive graphical display as well as downloadable and printable score list. This module performs retrieval of user scores as well as recommendations for best practices.

g) **Help Module:** this module provides help to the user on how to navigate through the system and perform system functions.

h) **Core application logic:** This module contains the logic that handles user requests by receiving, processes, and responding to those user requests. Additionally, this module allows inputs to the database, performs arithmetic computations of the security risk exposure index of the user in session, and returns results.

**i) System Databases:** The SREI platform maintains four working databases, namely; (i) users database that stores records of all registered users and acts as a reference by the authentication module on whether to allow user access or not, (ii) assessment questions database that stores a record as questions to be used for assessment, threshold scores per question, and corresponding recommendations, (iii) question categories database that stores a question categories depending on ISO 27001 control clauses, and (iv) the user assessment database that keeps a record of assessments done by the user and appends a timestamp to each assessment submitted successfully. This is the most active database in the SREI system.

### 5.2.6 System Components Interface

The SREI system was deployed as a web-based application therefore accessible through a web browser. The interface between the SREI system components was facilitated by use of navigation links to different modules as presented in figure 14 below.

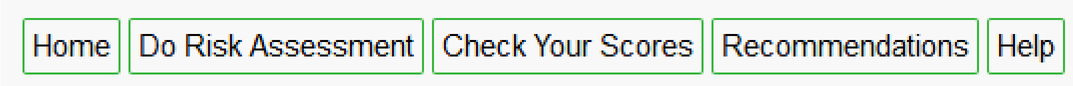


**Figure 13: SREI Prototype Navigation Panel**
**Source: Researcher (2017)**

### 5.3 System Design and Testing

This section presents a detailed logical design of the web-based model that was developed has four main players as discussed in section 5.3, namely; system users, administrators, domain registrars, and web hosts.

### 5.3.1 User Registration

This is the entry point to the SREI system that allows the user to register in order to be allowed access to the system functionalities. The system requires the user to provide such information to the system as; Full name, organization, username, email, and complex password. If the user provides all the required information required for the registration, the details are pushed to the database to be used by the login module for user authentication. The figure 15 below provides the flowchart of the registration process while figure 16 provides the graphical interface of the registration module.

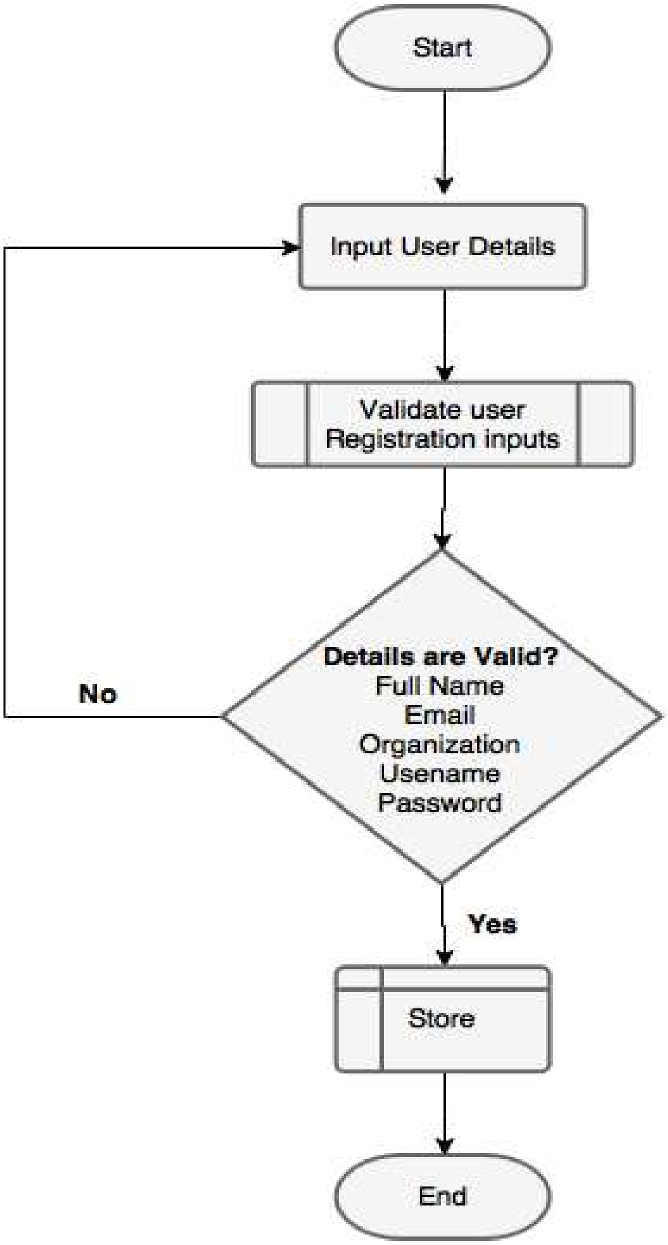
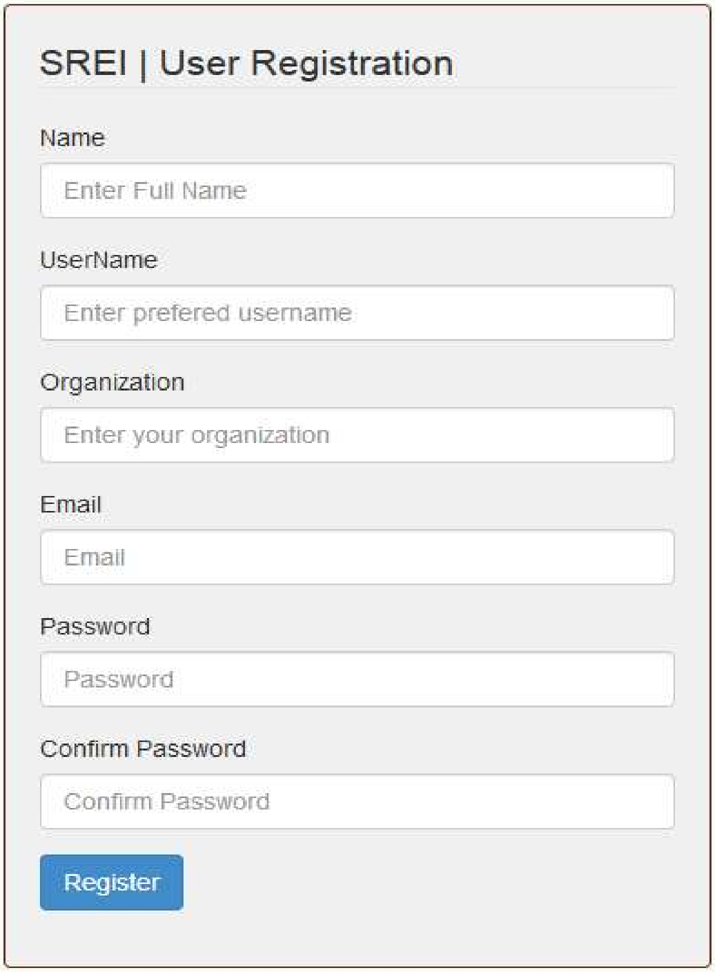


**Figure 14: Registration Process Flowchart**

**Source: Researcher (2017)**



SREI | User Registration

Name

Enter Full Name

UserName

Enter prefered username

Organization

Enter your organization

Email

Email

Password

Password

Confirm Password

Confirm Password

**Figure 15: Registration GUI**

**Source: Researcher (2017)**

### 5.3.2 Login Module

This module manages logins and sessions on users. It allows registered users to access system functionality by referring to users' database. If the user is not registered, it denies them access and prompts them to provide correct usernames, passwords, or register. Figure 17 below shows a flowchart representing the logic of the login system whereas figure 18 presents a graphical user interface of the login system.

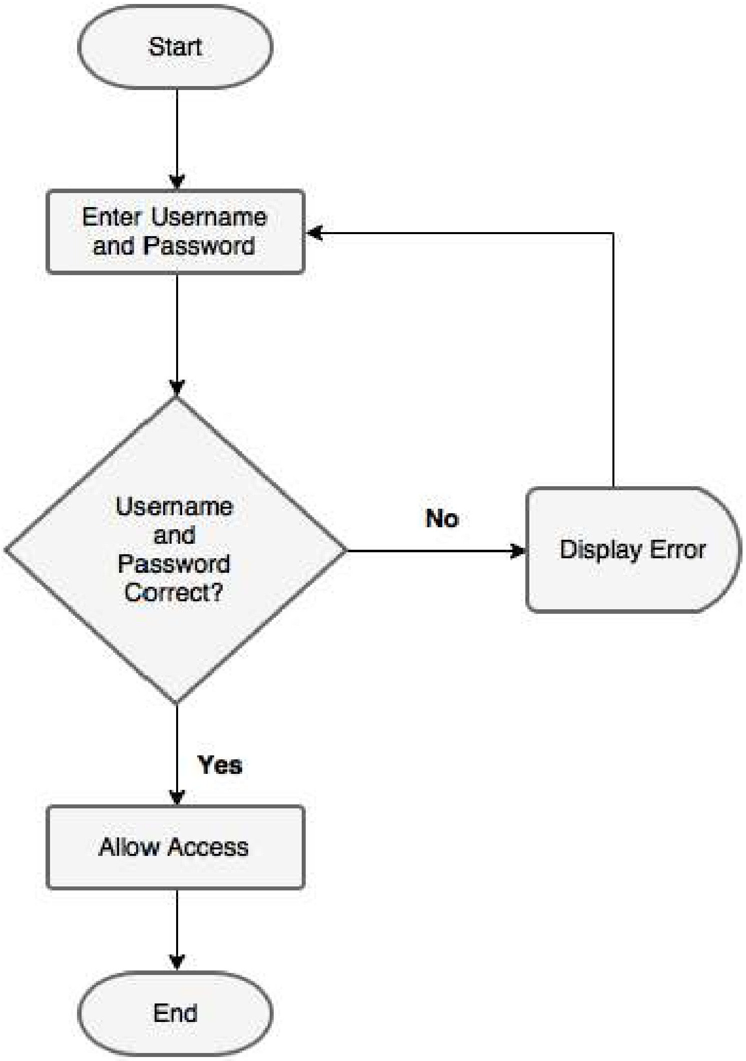


**Figure 16: Login Process Flowchart**

**Source: Researcher (2017)**

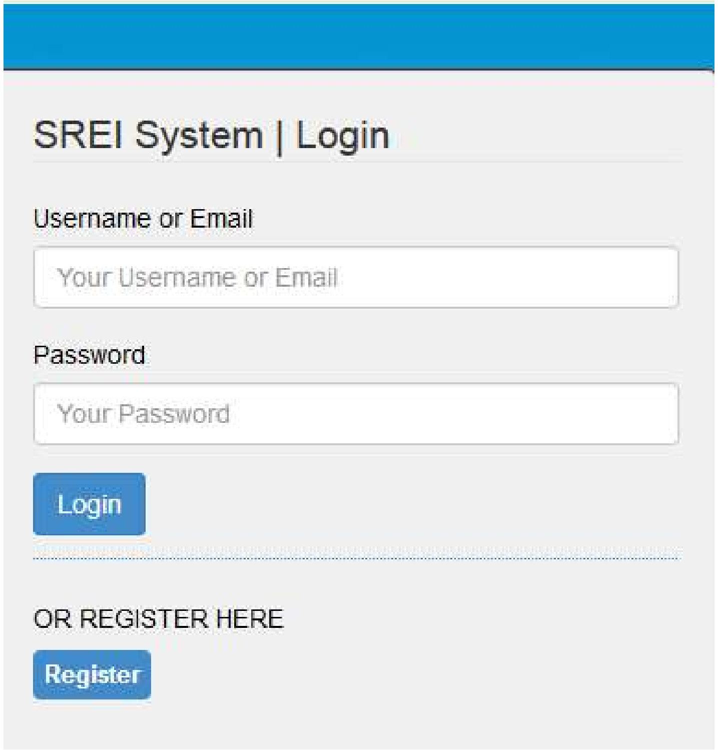


**Figure 17: Login GUI**

**Source: Researcher (2017)**

### 5.3.3 Risk assessment Module

This module allows the user to perform self-assessment for their organization by answering every assessment question in a Likert scale of 1 to 5. This module retrieves the questions from the database and presents it to the assessee in a Likert scale layout. Duly filled assessment form can be submitted to the database from where the Security Risk Exposure Index (SREI) will be computed. The Figure 19 below shows a flowchart presentation of the assessment logic whereas figure 20 is the presentation of the graphical user interface of the risk assessment module.

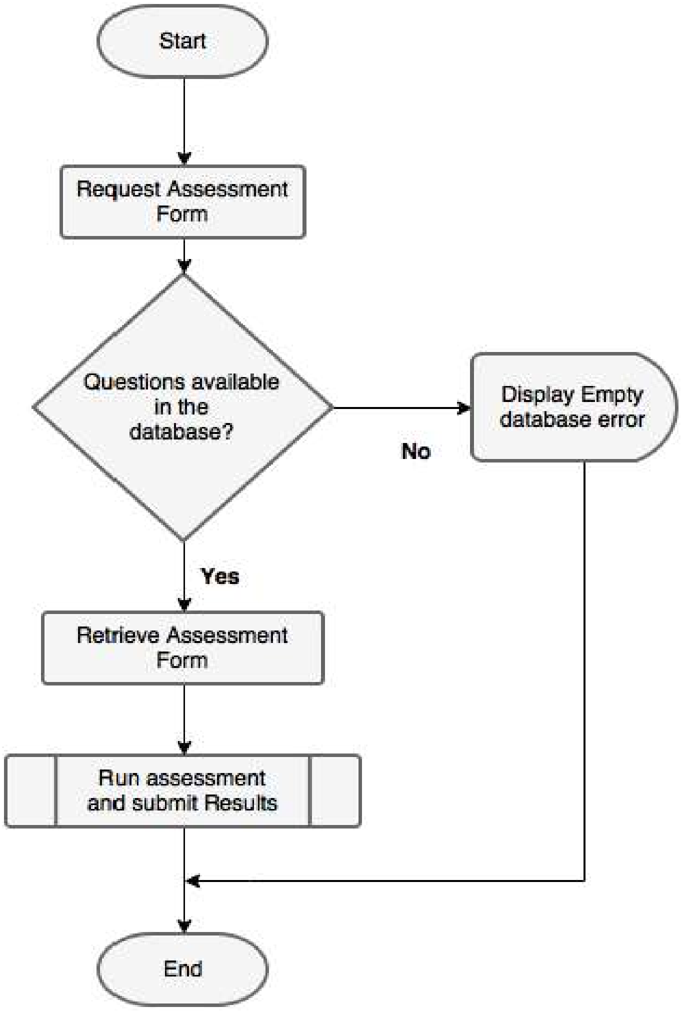
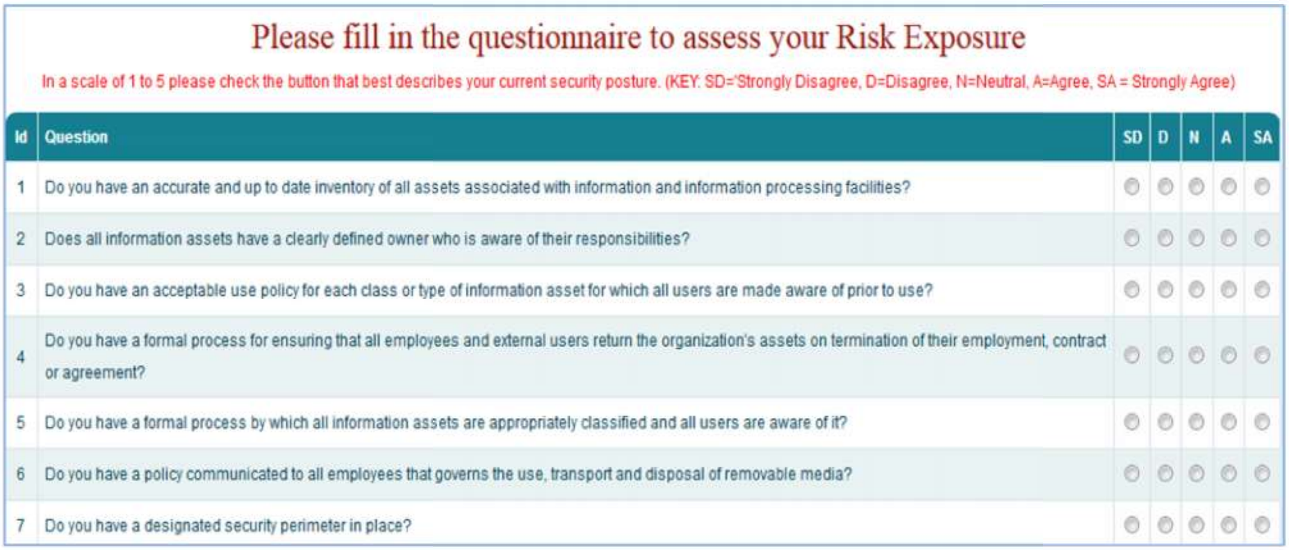

Start
Request Assessment Form
Questions available in the database?
No
Display Empty database error
Yes
Retrieve Assessment Form
Run assessment and submit Results
End

**Figure 18: Risk Assessment Flowchart**

**Source: Researcher (2017)**



Please fill in the questionnaire to assess your Risk Exposure

In a scale of 1 to 5 please check the button that best describes your current security posture. (KEY: SD='Strongly Disagree, D=Disagree, N=Neutral, A=Agree, SA = Strongly Agree)

| Id | Question | SD | D | N | A | SA |
|---|---|---|---|---|---|---|
| 1 | Do you have an accurate and up to date inventory of all assets associated with information and information processing facilities? | ○ | ○ | ○ | ○ | ○ |
| 2 | Does all information assets have a clearly defined owner who is aware of their responsibilities? | ○ | ○ | ○ | ○ | ○ |
| 3 | Do you have an acceptable use policy for each class or type of information asset for which all users are made aware of prior to use? | ○ | ○ | ○ | ○ | ○ |
| 4 | Do you have a formal process for ensuring that all employees and external users return the organization's assets on termination of their employment, contract or agreement? | ○ | ○ | ○ | ○ | ○ |
| 5 | Do you have a formal process by which all information assets are appropriately classified and all users are aware of it? | ○ | ○ | ○ | ○ | ○ |
| 6 | Do you have a policy communicated to all employees that governs the use, transport and disposal of removable media? | ○ | ○ | ○ | ○ | ○ |
| 7 | Do you have a designated security perimeter in place? | ○ | ○ | ○ | ○ | ○ |

**Figure 19: Risk Assessment GUI**

**Source: Researcher (2017)**

### 5.3.4 Assessment Scores Module

This component of the SREI platform allows the user to read back their assessment scores for all the questions submitted irrespective of the number of times the user has performed the assessment. Scores herein refers to the user's answers to ISO 27001 compliance checklist questions that in a range of 1 to 5. This module therefore allows the assessee to view a report of their responses to different questions and provide a mechanism for downloading the same in a portable document format that can be printed. In order to achieve this, this module groups the scores by the date of assessment. The figure 21 presents the assessment score retrieval logic in a flowchart. The figure 22 shows the graphical user interface presentation of the module.

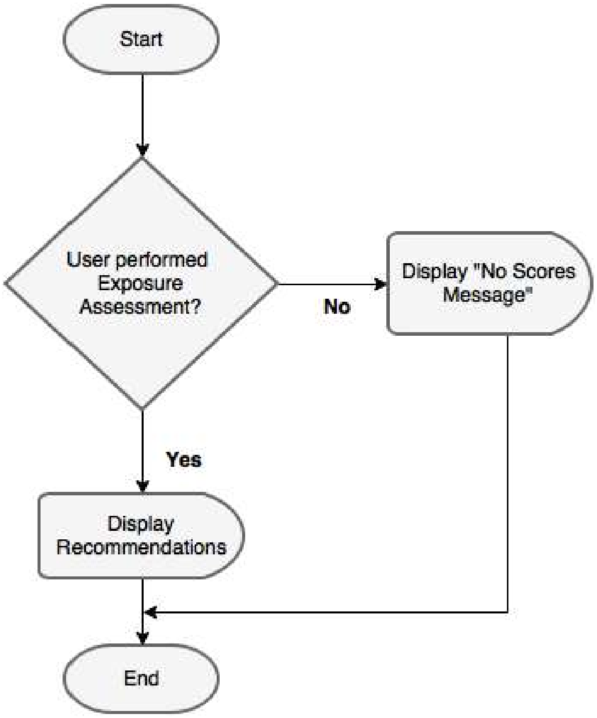
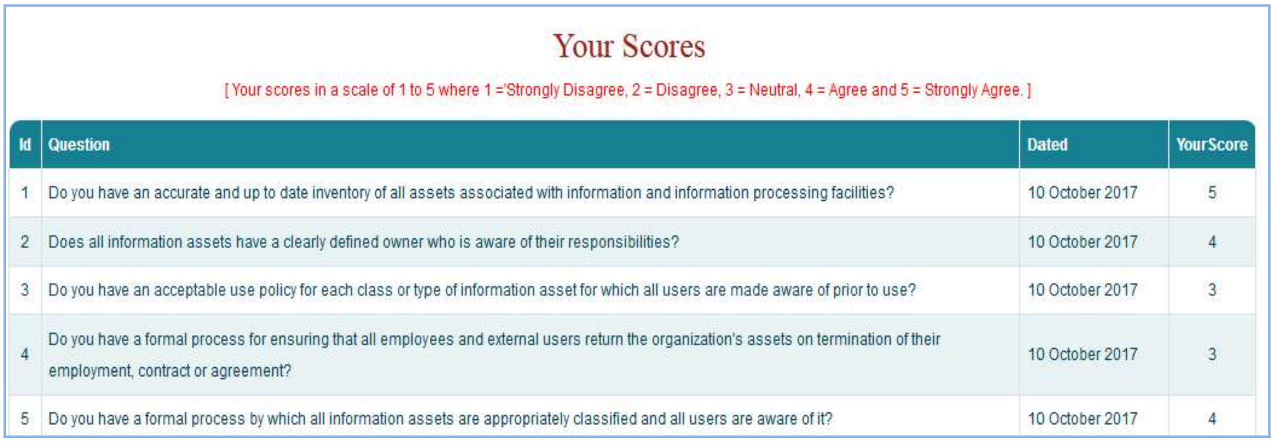

Start
User performed Exposure Assessment?
No
Display "No Scores Message"
Yes
Display Recommendations
End

**Figure 20: Score Flowchart**

**Source: Researcher (2017)**



Your Scores

[ Your scores in a scale of 1 to 5 where 1 ='Strongly Disagree, 2 = Disagree, 3 = Neutral, 4 = Agree and 5 = Strongly Agree. ]

| Id | Question | Dated | YourScore |
|---|---|---|---|
| 1 | Do you have an accurate and up to date inventory of all assets associated with information and information processing facilities? | 10 October 2017 | 5 |
| 2 | Does all information assets have a clearly defined owner who is aware of their responsibilities? | 10 October 2017 | 4 |
| 3 | Do you have an acceptable use policy for each class or type of information asset for which all users are made aware of prior to use? | 10 October 2017 | 3 |
| 4 | Do you have a formal process for ensuring that all employees and external users return the organization's assets on termination of their employment, contract or agreement? | 10 October 2017 | 3 |
| 5 | Do you have a formal process by which all information assets are appropriately classified and all users are aware of it? | 10 October 2017 | 4 |

**Figure 21: Scores GUI**

**Source: Researcher (2017)**

### 5.3.5 Recommendations Component

This component retrieves from the assessments database the recommendations that the user can implement in their organization to attain least risk exposure level and highest security risk maturity level. This module filters the recommendations for all the questions whose user assessment scores are below the thresholds and allows the user to download the recommendations in portable document format. The figures 23 and 24 shows logic flowchart and GUI presentations respectively.

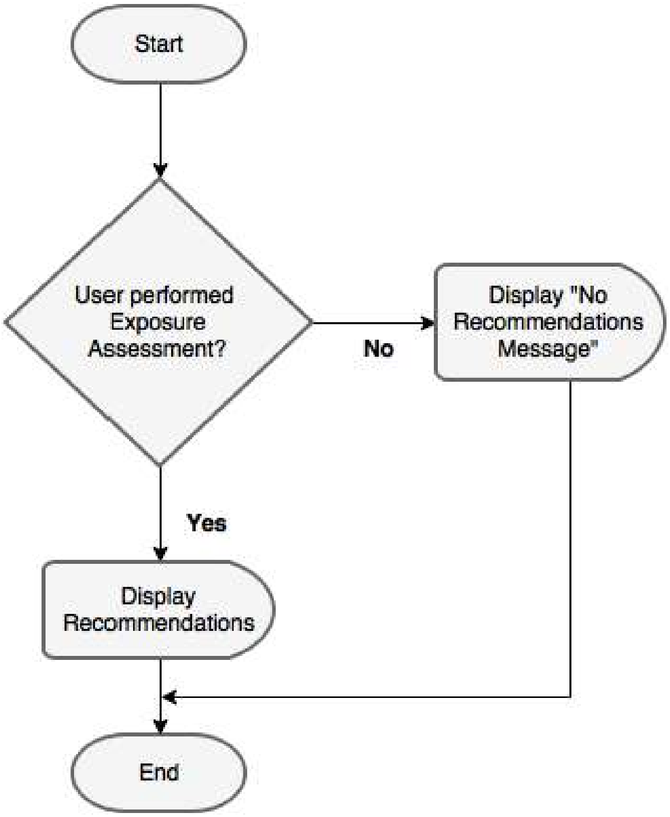
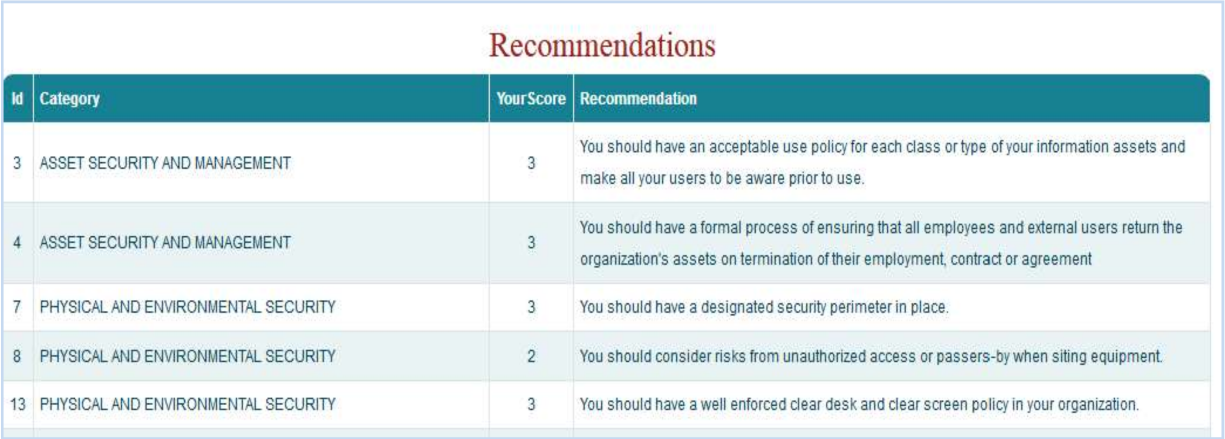

Start
User performed Exposure Assessment?
No
Display "No Recommendations Message"
Yes
Display Recommendations
End

**Figure 22: Recommendations Flowchart**

**Source: Researcher (2017)**



Recommendations

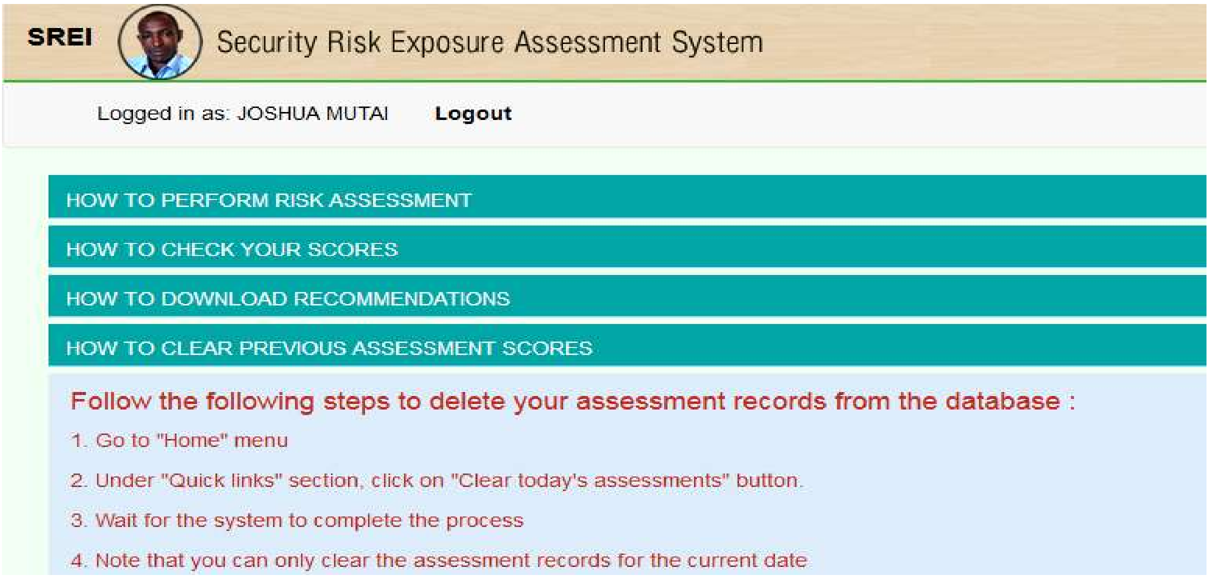
| Id | Category | YourScore | Recommendation |
|---|---|---|---|
| 3 | ASSET SECURITY AND MANAGEMENT | 3 | You should have an acceptable use policy for each class or type of your information assets and make all your users to be aware prior to use. |
| 4 | ASSET SECURITY AND MANAGEMENT | 3 | You should have a formal process of ensuring that all employees and external users return the organization's assets on termination of their employment, contract or agreement |
| 7 | PHYSICAL AND ENVIRONMENTAL SECURITY | 3 | You should have a designated security perimeter in place. |
| 8 | PHYSICAL AND ENVIRONMENTAL SECURITY | 2 | You should consider risks from unauthorized access or passers-by when siting equipment. |
| 13 | PHYSICAL AND ENVIRONMENTAL SECURITY | 3 | You should have a well enforced clear desk and clear screen policy in your organization. |

**Figure 23: Recommendation GUI**

**Source: Researcher (2017)**

### 5.3.6 Help Module

This module provides guidance to the user on how to navigate through the system and perform system functions. It presents help topic in a responsive collapsible panels called accordions. The figure 25 below presents a Graphical layout of the help interface.



SREI
Security Risk Exposure Assessment System
Logged in as: JOSHUA MUTAI
Logout
HOW TO PERFORM RISK ASSESSMENT
HOW TO CHECK YOUR SCORES
HOW TO DOWNLOAD RECOMMENDATIONS
HOW TO CLEAR PREVIOUS ASSESSMENT SCORES

Follow the following steps to delete your assessment records from the database :

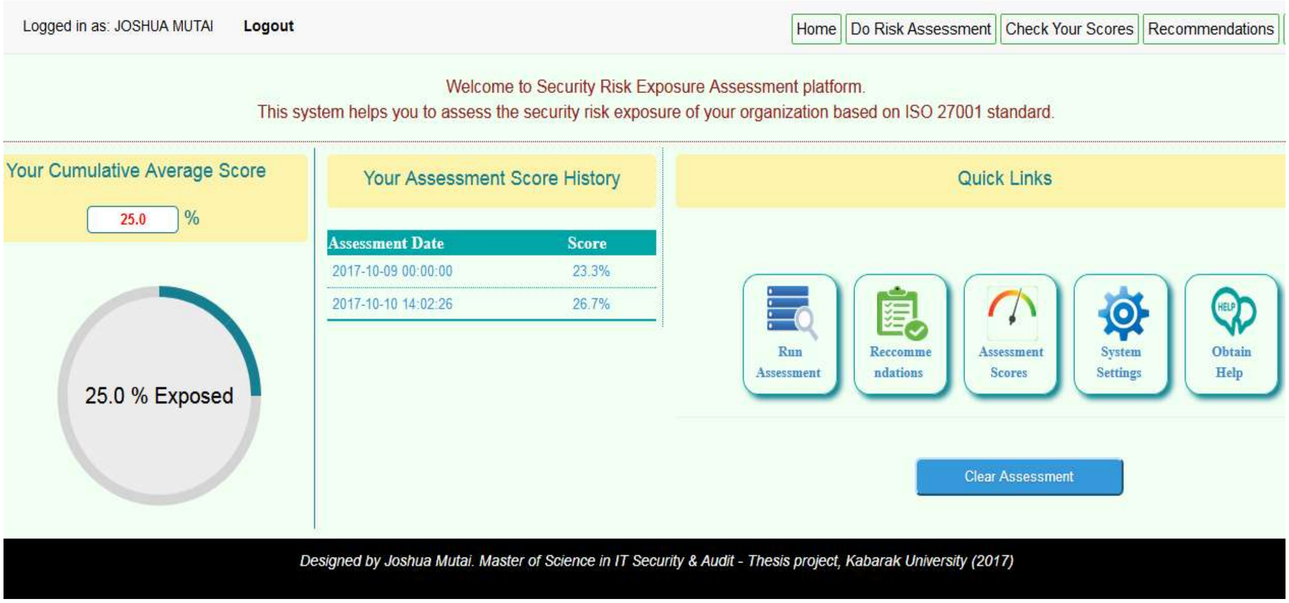
1. Go to "Home" menu
2. Under "Quick links" section, click on "Clear today's assessments" button.
3. Wait for the system to complete the process
4. Note that you can only clear the assessment records for the current date

**Figure 24: Help GUI**

**Source: Researcher (2017)**

### 5.3.7 Home Display

This component presents a responsive home page that allows the user to make quick navigations, view graphical presentation of their cumulatively computed SREI, their assessment history by date and corresponding computed SREI. The user at this stage can opt to clear assessments scores even though deletion is only limited to that current date of assessment. That means that the user cannot delete assessment scores for previous dates because they will be needed for comparison. The figure 26 presents a graphical user interface layout of home display component. At this component, the system allows the user to view their cumulative SREI scores. For instance, in the case of the cumulative average score for the use is in the figure 26 below is 25 percent.



Logged in as: JOSHUA MUTAI

Welcome to Security Risk Exposure Assessment platform.
This system helps you to assess the security risk exposure of your organization based on ISO 27001 standard.

Your Cumulative Average Score

25.0 %

25.0 % Exposed

Your Assessment Score History

| Assessment Date | Score |
|---|---|
| 2017-10-09 00:00:00 | 23.3% |
| 2017-10-10 14:02:26 | 26.7% |

Designed by Joshua Mutai. Master of Science in IT Security & Audit - Thesis project, Kabarak University (2017)

**Figure 25: Home GUI**

**Source: Researcher (2017)**

### 5.3.8 Entity Relationship Diagram

The entity relationship diagram for the SREI system is presented in figure 27. It contains 4 database tables for storing four main types of information;

**a)** User registration and authentication information: user_id, username, full name, email, organization, and password (MD5 cryptographic hash)

**b)** Question categories information: category_id, category name

**c)** System Questions information: Category_id, question_id, question, recommendation, threshold score

**d)** Assessment information: user_id, question_id, score, assessment date

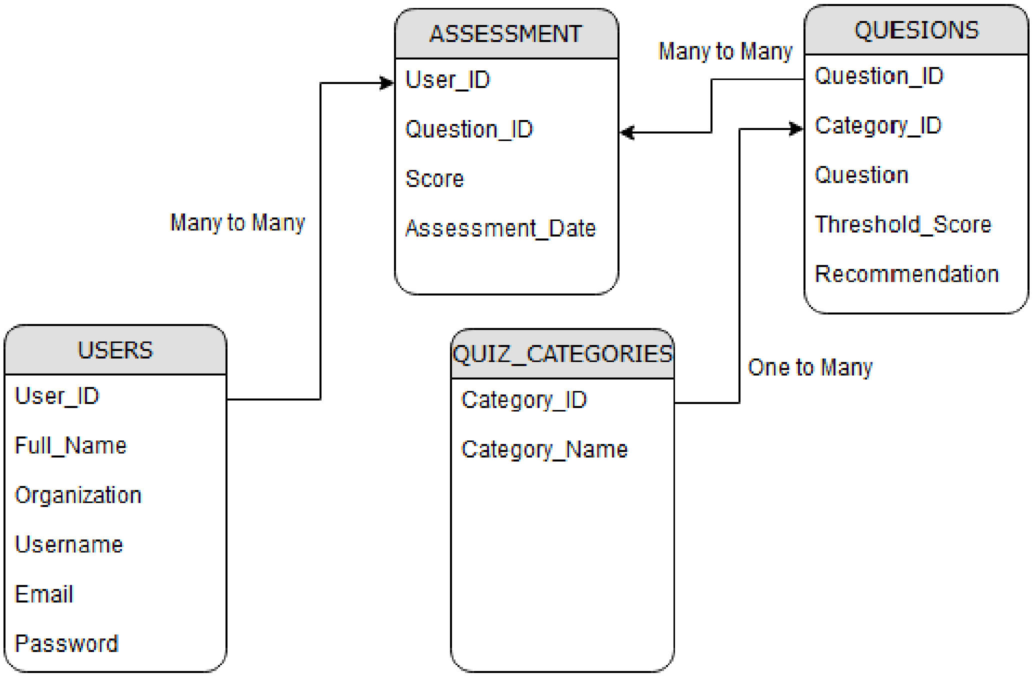


**Figure 26: Entity Relationship Diagram**

**Source: Researcher (2017)**

### 5.3.9 Proof of Concept

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

## 5.4 System Evaluation

In an attempt to determine the extent to which the designed model achieved the preset objectives, the prototype was evaluated using IT-Systems as such Goal-based evaluation approach presented in section 3.7 (Youker, 2014). The goal-based evaluation using IT-Systems as such was done as presented in table 11 below;

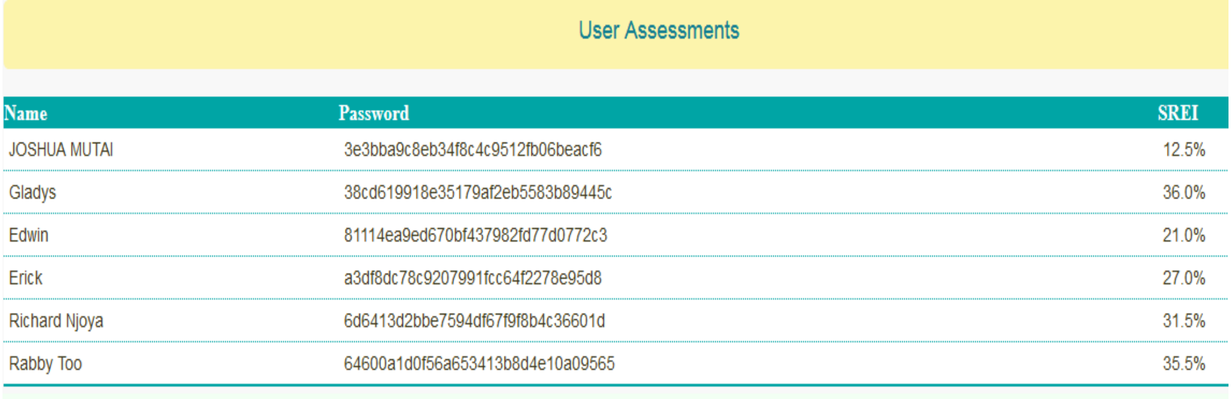
**Table 5.1: IT System as Such' Goal Based Evaluation**

| | Objective | | Evaluation Results |
|---|---|---|---|
| **1.** | **User registration:** The prototype was to allow capturing of user details, validating user inputs, encrypting user passwords. I was also expected to store validated user details in a database | **a)** | The prototype was able to take user details from the user and validate the inputs for instance, it enforces password complexity and standard email formats. |
| | | **b)** | The prototype was able to apply MD5 cryptographic function to hash user passwords. |
| | | **c)** | The prototype was able to store validated user registration details in MySQL database. |
| **2.** | **User login and Authentication:** The prototype was expected to read prompt user to provide login credentials before being allowed to access the system components. | **a)** | The prototype prompted user for login credentials and matches with the ones stored in the database. |
| | | **b)** | The prototype further allowed the user access whose username or email and password matches those stored in the database. |
| **3.** | **Risk Assessment and Submission:** The prototype was to retrieve assessment questions from the database and present to the user in a likert scale layout. It was also to allow the user to submit duly filed assessment form to the database | **a)** | The prototype was able to retrieve assessment questions and from the database and present them in an easy-to-use likert scale format for the user. |
| | | **b)** | It allowed the user to submit score from a duly filled assessment form into the database. |
| **4.** | **SREI Computation:** The prototype was expected to compute the exposure index using submitted user scores and present the results to the | **a)** | The prototype was able to read the user scores from the database from which it computed SREI. |
| | | **b)** | It provided an easy-to-use Graphical |

| | | |
|---|---|---|
| | user in an easy-to-read graphical view. | presentation of the computed SREI results using JQUERY circular status bar. |
| **5** | **Scores and recommendations:** The prototype was expected to retrieve scores and recommendations thereof then display the results on web page and allow the user to download the output into a portable and printable document format. | **a)** The prototype was able to retrieve the scores as well as recommendations from the database and present in web pages<br>**b)** It was also able to allow the user to download the output into a portable document format that can be printed. |

## 5.5 Verification and validation of the model

The SREI model was designed, hosted with domain registrar and host then users were allowed to register, login and perform their independent security risk assessment using the system. It was noted that the system had captured the details of the users, encrypted their passwords using MD5 hash function. The records of user scores were also stored in the database successfully with timestamps attached to each assessment row. In addition, reports of SREI computation for all the users that logged in and submitted their scores could be seen with the time of assessment attached. The system could successfully retrieve information of recommendations based on user assessment scores. The figure 28 below shows an interface of admin view of user assessment records with computed SREI scores and date of assessments



User Assessments

| Name | Password | SREI |
|---|---|---|
| JOSHUA MUTAI | 3e3bba9c8eb34f8c4c9512fb06beacf6 | 12.5% |
| Gladys | 38cd619918e35179af2eb5583b89445c | 36.0% |
| Edwin | 81114ea9ed670bf437982fd77d0772c3 | 21.0% |
| Erick | a3df8dc78c9207991fcc64f2278e95d8 | 27.0% |
| Richard Njoya | 6d6413d2bbe7594df67f9f8b4c36601d | 31.5% |
| Rabby Too | 64600a1d0f56a653413b8d4e10a09565 | 35.5% |

**Figure 27: Model Verification and Validation**

**Source: Researcher (2017)**

## 5.6 Scalability and other Areas of Application

Although the SREI system design was scoped to the SACCOs in Kenya and based on only six ISO 27001-assessment controls, it has the potential of being scaled to include all the elevenISO 27001 controls and applied to organizations other than the SACCOs and countries other than Kenya. A mobile application could also be developed using android and/or iOS. Scalability was achieved by using the following SQL code snippet;

```
$sql = “SELECT 100-round (sum (score)/ (COUNT (questionid)*5)*100, 1) FROM
assessment where userid=$user_id”;
```

This allows for expansion of assessment scope to accommodate questions more than the 40 used in this study. It gets the sum of all questions, divides by the product of the number of questions and the highest possible score (5), converts to percentage then rounds off the results to one decimal point.

# CHAPTER SIX

# CONCLUSIONS AND RECOMMENDATIONS

## 6.1 Introduction

This chapter presents the conclusions on the design of mathematical model and the web-based model. It concluded on how every objective of the research was achieved, areas for further study and the recommendations.

## 6.2 Conclusions

This study aimed at solving the underlying problem in Kenyan Savings and credit cooperative societies of operating on the cyberspace with less investment towards security controls and the ever-increasing threat landscape targeting their ever-increasing asset base. Therefore, this study was based on the need to have a customized SREI model to assist the SACCOs to determine their risk exposure posture based on ISO 27001 standards as a benchmark for information security.

A solution was delivered through the design of SREI model, which is an easy-to-use, accessible and affordable web application. A review of other existing models was done extensively and gabs were established on the failure of those technologies to ride on well-established frameworks to deliver reliable assessments platforms. This therefore prompted the need for a tailored model based on ISO 27001 standards as a backbone for reliable security strategies to help the SACCO in Kenya determines their exposure indices. The designed SREI solution was able to effectively handle user registration, user authentication, risk assessment, and reports access for scores and recommendations. More detailed conclusions on whether the specific objectives were achieved are discussed herein below in sections 6.2.1 to 6.2.3.

### 6.2.1 Research Question 1: What are the critical security risks factors affecting savings and Credit Cooperative societies in Kenya based ISO 27001 standard?

The study established that the most critical security risk factors affecting Savings and Credit Cooperative Societies in Kenya from the 11 of ISO 27001 factors are; physical and environmental security, Human Resource security, asset management and security, system security, access control, and compliance. These factors contributed the most to the exposure of the SACCOs to security threats. Although the SACCOs in Kenya were required to pay attention to all the 11 ISO 27001 control factors, more attention needed to be put on the 6 factors established by this study if minimum exposure index was to be realized. Therefore, the SREI system was necessary in helping the SACCOs to establish their exposure index and recommended controls to secure their organizations

### 6.2.2 Research Question 2: How will the model for computing Security risk exposure index in savings and credit cooperative in Kenya be developed?

A linear mathematical approach was used to develop Security Risk Exposure index (SREI) model for computing Security Risk Exposure index of an organization. The weights used in the mathematical model were the regression weights established by the study while security variables were the scores of information provided by the based on ISO 27001 standard checklists. Therefore, the design of Security Risk Exposure index System relied heavily upon the ISO 27001 standard of IT Security best practices.

### 6.2.3 Research Question 3: How will the prototype of a web-based application for computing SREI are implemented?

The prototype for computing SREI was designed as a web based application using PHP as a server-side language, JQuery for frontend interactions, and MySQL as a database engine. The model has a database for storing assessment questions information, assessment scores information and system users' information. There were well-designed integrations between the database and the user interface. The model relies on the assessment information stored in the database to compute and determine security exposure of the assessee. The model displays the results of Security Risk Exposure Index in a graphical and easy-to-read graphical view. Based on the same score, information, the model can present the user with recommendations for best practices.

### 6.2.4 Research Question 4: Can the Model Compute SREI?

The model for computing SREI was designed and made available online by hosting with web host. Users registered and logged into the system then performed system activities, which included, running assessments and submitting scores, viewing their scores, reading their exposure index computed by the model, and retrieving recommendations. In all these activities, the system was verified to have performed the intended functionalities. User details were stored in the database after validation and passwords encrypted. User scores were also stored after validation and used to compute SREI and retrieve recommendations accurately.

### 6.3 Areas of Further Research

During the course of this research study, areas of further study were established. This includes, but not limited to; the need to determine further limitations and challenges of the perceived ease-of-use of the SREI system and how to improve, establish how other international standards focused towards risk management in organizations can be incorporated to increase the reliability and robustness of the SREI system. The following sections 6.3.1 to 6.3.4 present further details on areas of further study.

#### 6.3.1 SREI Commercialization

More time and resources need to be further expended on this study in order to achieve a commercially viable service that runs on web browsers, as mobile android or iOS app.

#### 6.3.2 Risk versus Perceived benefits of SREI

In as much as the SREI system is perceived to have profound benefits to the users in helping to determine security risk exposure index, there could be challenges especially on the sincerity of the users to provide accurate information as pertains their present risk posture for fear of status disclosure. It is therefore prudent to expend more time to further this study to establish the challenges and risks of SREI System.

#### 6.3.3 Security Reinforcement of Web-based SREI System

On the onset, SREI system allows the users to register by providing their details for which the system will take in and store in its database as provided by the user. The challenge sets in when users provide incorrect information during registration. This can be difficult for the regulating agencies to ascertain the authenticity of the said users. More time and resources is needed to further this study to establish a more sound management of registration process for organizations, and involvement of government regulating authorities in using the system for oversight.

### 6.3.4 User Trust

There is need to further this study to establish the adoption and trust of SREI system by organizations given that those organizations have to provide somewhat sensitive information regarding security posture of their establishments.

## 6.4 Recommendations

This section presents the recommendations that this study is proposing.

### 6.4.1 Central Management

Although the SREI system was designed and hosted online where users can access, register, login, and utilize system functionalities, the researcher recommends the need to have a central management unit. The unit should probably a government agency or a regulatory body that manage database centrally, own the registration process so that anonymous users may not register, validate users of the system, and protect sensitive information that is provided by the organizations.

### 6.4.2 Enforced Compliance

SACCO Societies Regulatory Authority (SASRA) needs to incorporate this model in their oversight role of the SACCOs in Kenya. SASRA can enforce the requirement for SACCOs to perform their online security risk assessments on monthly basis alongside other regulatory reports they receive monthly from licensed SACCOs. This will help monitor the improvement or non-improvement of SACCOs in compliance with ISO 27001 standard requirements for security.

# REFERENCES

Alberts, C. J & Dorofee, A. (2002). *Managing information security risks: the OCTAVE approach*. Addison-Wesley Longman Publishing Co., Inc.

Ashenden, D. (2008). Information security management: A human challenge? *Information security technical report*, 13(4), 195-201.

Atavachi, B. S. (2013). *Effect of electronic banking on financial performance of deposit taking micro-finance institutions in Kenya* (Doctoral dissertation, University of Nairobi).

Bauer, J. M. & Dutton, W. H. (2015). The New Cybersecurity Agenda: Economic and Social Challenges to a Secure Internet. Retrieved 22 March 2018, from: http://documents.worldbank.org/curated/en/689851467991972707/The-new-cybersecurity-agenda-economic-and-social-challenges-to-a-secure-internet

Biscoe, C. (2017). *Top 10 threats to include in an ISO 27001 risk assessment. IT Governance Blog*. Retrieved 4 May 2017, from https://www.itgovernance.co.uk/blog/top-10-threats-to-include-in-an-iso-27001-risk-assessment/

Bonnette, C. (2003). Assessing Threats to Information Security in Financial Institutions. *GSEC Certification Assignment Paper, Information Security Reading Room, SANS Institute*, *9*.

Bradshaw, S. (2015). Combating Cyber Threats: CSIRTs and Fostering International Cooperation on Cyber security. *Global commission on internet governance paper series: 23(1)*

Brauch, H. G. (2011). Concepts of security threats, challenges, vulnerabilities and risks. In *Coping with Global Environmental Change, Disasters and Security* Springer Berlin Heidelberg. pp. 61-106.

Brewer, N. & Nash, M. (2010). *Insights into the ISO 27001 Annex A.* Retrieved 22 March 2018, from *http://www.gammassl.co.uk/research/27001annexAinsights.pdf*

Bulgurcu, B., Cavusoglu, H. & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS quarterly*, 34(3), 523-548.

Byres, E. & Lowe, J. (2004). The myths and facts behind cyber security risks for industrial control systems. *In Proceedings of the VDE Kongress* 116, pp. 213-218.

Camarinha-Matos, L. M. (2009). Scientific research methodologies and techniques. Retrieved 22 March 2018, from https://www.hutech.edu.vn/khoacntt/attachments/article/3088/SRMTunit1.pdf

Calder, A. & Watkins, S. (2008). *IT governance: A manager's guide to data security and ISO 27001/ISO 27002*. Kogan Page Ltd..

*Cambridge product* (2011). *Cambridge essential English dictionary*. (1st ed.). Cambridge.

Chahayo, S. A., Bureti, F., Juma, M. M. & Aketch R.A. (2013). Analysis of Financial Mismatch in Co-Operative Societies: A Case of Kakamega County, Kenya. *International Journal for Management Science and Technology*, *1*(5).

Chatzipoulidis, A. & Mavridis, I. (2009). Evolving Challenges in Information Security Compliance. *In MCIS* (p. 75).

Chua, C. K., Leong, K. F., & Lim, C. S. (2003). *Rapid Prototyping: Principles and Applications* 2nd Ed. (with Companion CD-ROM) (Vol. 1). World Scientific Publishing Co Inc.

Cole, E. & Ring, S. (2005). *Insider threat: Protecting the enterprise from sabotage, spying, and theft*. Syngress.

Cronholm, S. (2004). Information Systems Evaluation-adding process descriptions to six evaluation types. In *the Proceedings of the 11th European Conference on Information Technology Evaluation (ECITE'04). Royal Netherlands Academy of Arts and Sciences, Amsterdam* (pp. 11-12).

Cruz, B. (2013). *Vulnerability, exposure, threat and risk terms*. *Belencruz.com*. Retrieved 6 March 2017, from http://belencruz.com/2013/04/vulnerability-exposure-threat-and-risk-terms/

Curtis, P. & Carey, M. (2012). *Risk assessment in practice*. New York: Committee of Sponsoring Organizations of the Treadway Commission. COSO.

Common Vulnerabilities and Exposures (CVE)  (2017). *CVE -Terminology*. *Cve.mitre.org*. Retrieved 2 April 2017, from https://cve.mitre.org/about/terminology.html

Diaz-Gomez, P. A., ValleCarcamo, G. & Jones, D. (2010). Internal vs. external penetrations: A computer security dilemma. In *Proceedings of the 2010 International Conference on Security & Management*. . Retrieved 22 March 2018, from *http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.218.1712&rep=rep1&type=pdf*

Dictionary, B. (2012). Business dictionary. *Retrieved April*, *17*, 2017. https://doi.org/10.1016/j.sbspro.2014.04.212

Dunkelberger, D. (2017). *Top 5 Cyber security Challenges Facing Financial Service Institutions*. I.S. Partners, LLC. Retrieved 1 November 2017, from https://www.ispartnersllc.com/blog/top-5-cybersecurity-challenges-facing-financial-service-institutions/

Farlex, I. N. C. (2009). The free dictionary. *Retrieved June*, *28*, 2012.https://www.thefreedictionary.com/

Fomin, V. V., Vries, H. & Barlette, Y. (2008). ISO 27001 information systems security management standard: Exploring the reasons for low adoption. In Proceedings of the third European conference on Management of Technology (EuroMOT). *Retrieved April*, *17*, 2017. https://pdfs.semanticscholar.org/2be0/f60530378b5595cb6138be39a13c0fa60e13.pdf

Franqueira, V. N., van Cleeff, A., van Eck, P., & Wieringa, R. (2010). External insider threat: A real security challenge in enterprise value webs. In *Availability, Reliability, and Security, 2010. ARES'10 International Conference on* (pp. 446-453). IEEE.

Global Economic Crime Survey 2016. (2016). *PwC*. Retrieved 1 April 2017, from http://www.pwc.com/crimesurvey

Guguyu, O. (2016). *Kenya: Central Bank Puts Firms on High Alert Over Cyber Attacks*. *allAfrica.com*. Retrieved 6 April 2017, from http://allafrica.com/stories/201605251074.html

International Cooperative Alliance (ICA) (2005). International Cooperative Alliance Statement of the Co-operative identity, values & principles. Retrieved from: http://old.ica.coop/en/whats-co-op/co-operative-identity-values-principles.

ISO/IEC, (2005). ISO/IEC 27001:2005 *Information Technology. Security Techniques. Specification for an Information Security Management System.* Geneva, Switzerland: ISO/IEC.

ISO 27001 Annex A – An overview of 2013 revision. (2017). 27001 Academy. Retrieved 13 May 2017, from https://advisera.com/27001academy/knowledgebase/overview-of-iso-270012013-annex-a/

Jouini, M., Rabai, L. B. A. & Aissa, A. B. (2014). Classification of security threats in information systems. *Procedia Computer Science*, *32*, 489-496.

Julisch, K. (2009). *Security compliance: the next frontier in security research. In Proceedings of the 2008 workshop on New security paradigms* (pp. 71-74). ACM.

Kigen, P. M., Muchai, C., Kimani, K., Mwangi, M., Shiyayo, B., Ndegwa, D. & Shitanda, S. (2015). *Kenya Cyber Security Report 2015*. Serianu Limited.

Kigen, P. M., Muchai, C., Kimani, K., Mwangi, M., Shiyayo, B., Ndegwa, D. & Shitanda, S. (2016). *Kenya Cyber Security Report 2016*. Serianu Limited.

Koduk, S. C. (2015). *The effect of electronic banking on financial performance of savings and credit cooperative societies in Nairobi county* (Doctoral dissertation, University of Nairobi).

Krutz, R. L. & Vines, R. D. (2003). *The CISSP prep guide*. John Wiley & Sons, Inc..

KPMG. (2016). *KPMG in India launches 'Cyber KARE'. KPMG*. Retrieved 16 April 2017, fromhttps://home.kpmg.com/in/en/home/media/press-releases/2016/03/cyber-kare.html

Maina, S. (2017). *REPORT: African Countries Lost At Least 2 Billion Dollars to Cyberattacks in 2016*. *Techweez*. Retrieved 18 March 2017, from http://www.techweez.com/2017/04/11/africa-cyberattacks-reports-2016/

Mateski, M., Trevino, C. M., Veitch, C. K., Michalski, J., Harris, J. M., Maruoka, S., & Frye, J. (2012). *Cyber threat metrics*. Sandia National Laboratories.

Mehmood, F. & Rafique, R. (2010). *Management of operational risks related to information security in financial organizations* Retrieved 18 March 2017. *http://www.diva-portal.org/smash/get/diva2:325089/fulltext01.pdf*

Nakrem, A. (2007). Managing information security in organizations: a case study (Master's thesis, Høgskolen i Agder).

National Institute of Standards and Technology (NIST), & United States of America. (2014). *Framework for Improving Critical Infrastructure Cybersecurity.* Retrieved 18 March 2017. *http://go.secureworks.com/state-and-local-governments-take-a-risk-based-approach-to-cybersecurity?SE-CO-2.1.35N&LS=PPC&LSP=NALE&SE-CO-2.1.35N&LSF=SE*

NIST, G. S., Goguen, A., & Fringa, A. (2002). Risk Management Guide for Information Technology Systems. *Recommendations of the National Institute of Standards and Technology*. Retrieved 18 March 2017 https://www.archives.gov/files/era/recompete/sp800-30.pdf

Northcutt, S. (2009). *Security Controls*. *Sans.edu*. Retrieved 8 April 2017, from https://www.sans.edu/cyber-research/security-laboratory/article/security-controls

Nyawanga, J. O. (2015). *Meeting the challenge of cyber threats in emerging electronic transaction technologies in in Kenyan banking sector* (Doctoral dissertation, University of Nairobi).

Open University, (2013). *An Introduction to Information Security*. Walton Hall,Milton Kaynes MK7 6AA: Open University.

PWC. (2016). *Global Economic Crime Survey 2016*. *PwC*. Retrieved 24 March 2017, from http://www.pwc.com/crimesurvey

Rudis, B., Beardsley, T., & Harts, J. (2017). *Security Research: National Exposure Index*. *Rapid7*. Retrieved 5 April 2017, from https://information.rapid7.com/national-exposure-index.html

Rufi, A. (2007). *Network security 1 and 2 companion guide*. Indianapolsis, Ind.: Cisco Press.

Ryan, V. (2013). TESTING AND EVALUATING A PROTOTYPE - WHY?. Technologystudent.com. Retrieved 2 April 2017, from http://www.technologystudent.com/despro_flsh/evalintegr1.html

SACCO Societies Regulatory Authority (SASRA). (2015a). *Sacco Supervision Report:* Deposit Taking SACCOs.  In house Publication.

SACCO Societies Regulatory Authority (SASRA). (2015b). *Guideline on Risk Management Practices for Deposit Taking SACCOs*. In house Publication.

Sabale, R. G. & Dani, A. R. (2012). Comparative study of prototype model for software engineering with system development life cycle. *IOSR Journal of Engineering*, 2(7), 21-24.

Schweizerische, S. N. V. (2013). Information technology-Security techniques-Information security management systems-Requirements. *ISO/IEC International Standards Organization.* Retrieved 2 April 2017 *https://trofisecurity.com/assets/img/iso27001-2013.pdf*

Susanto, H., Almunawar, M. N. & Tuan, Y. C. (2012). Information security challenge and breaches: novelty approach on measuring ISO 27001 readiness level. *International Journal of Engineering and Technology. IJET Publications UK*, *2*(1).

Tipton, H. F. & Nozaki, M. K. (2012). *Information Security Management Handbook*, 6. Auerbach Publications.

Verizon. (2016). *Enterprise Technology Solutions & Managed IT Services*. *Verizon Enterprise Solutions*. Retrieved 10 April 2017, from http://www.verizonenterprise.com/

Waswa, C. M. (2013). *Effect of regulatory controls on interest rates of deposit taking savings and credit co-operative societies in Nairobi County* (Doctoral dissertation, University of Nairobi).

Wilson, M. & Hash, J. (2003). Building an information technology security awareness and training program. *NIST Special publication*, 800(50), 1-39.

Youker, B. W. (2014). Goal-free Evaluation and Goal-Based Evaluation. *The Foundation Review 5(4) 50-61.*

# Appendix A: Questionnaire

I am a Master of Science (IT Security and Audit) student of Kabarak University carrying out a research on "A model to determine risk exposure index in Savings and Credit Cooperative Societies in Kenya". This is to humbly request you to answer the questions outlined here below as truthfully as you can. Please note that the information you provide will be used only for this academic research and will be protected by strict ethical standards of anonymity.

## PART A: Basic Information

*Please tick the most appropriate answer in this section*

1. ***Which one of the following best describes your position in the SACCO?***

(i) Full time Employee **[ ]** (ii) Part time employee **[ ]**

(iii) Contractor **[ ]** (iv) Partner **[ ]**

(v) Vendor **[ ]** (vi) Other **[ ]**

2. ***What comprises the biggest membership of your SACCO***

(i) Teachers **[ ]** (ii) Farmers **[ ]**

(iii) Workers **[ ]** (iv) Doctors **[ ]**

(v) Uniformed forces **[ ]** (vi) Business **[ ]**

## PART B: SPECIFIC QUESTIONS

3. In a scale of 1 to 5, to what extend do you think the following 11security risk factors are critical to your SACCO? (***KEYS**: **1**=Not Very Critical, **2**=Not Critical, **3**=Neutral, **4**=Critical, **5**=Very Critical**)***

| **NO** | **Question** | **1** | **2** | **3** | **4** | **5** |
|---|---|---|---|---|---|---|
| **1** | Security Policy | | | | | |
| **2** | Physical and Environmental Security | | | | | |
| **3** | Human Resource Security | | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| **4** | Asset Management | | | | | |
| **5** | Communication & Operations Management | | | | | |
| **6** | Organization of Information Security | | | | | |
| **7** | System Security | | | | | |
| **8** | Access Control | | | | | |
| **9** | Information Security Incident Management | | | | | |
| **10** | Business Continuity Management | | | | | |
| **11** | Compliance | | | | | |

## PART C: QUESTIONS

In the scale of 1 to 5, please tick the most appropriate answer to the questions here below in relation to management and Asset security, Physical Security, System Security, Human resources security, access controls, and Compliance in your SACCO. (***KEYS***: ***1****=strongly disagree*, ***2****=Disagree*, ***3****=Neutral*, ***4****=Agree*, ***5****=strongly Agree)*

### 4. ASSET SECURITY AND MANAGEMENT

| **NO.** | **Questions** | **1** | **2** | **3** | **4** | **5** |
|---|---|---|---|---|---|---|
| 1 | There is an up-to-date inventory of all assets in form of information and information processing facilities. | | | | | |
| 2 | There are clearly defined owners for all information assets. Owners know their responsibilities. | | | | | |
| 3 | Acceptable-use-policy applies for each type / class of information asset and all users are conscious of it before they use. | | | | | |
| 4 | There is a formal process for ensuring that all employees and external users return institution's assets upon end of contract, agreement, or employment. | | | | | |
| 5 | There is a formal process through which all information is appropriately categorized and all users of information assets understand it. | | | | | |
| 6 | There is a policy governing use, transport, and disposal of removable media and all employees are aware of it. | | | | | |

**PHYSICAL AND ENVIRONMENTAL SECURITY**

| NO. | Questions | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| 1 | The organization has installed a designated security perimeter. | | | | | |
| 2 | Risks from unauthorized access or passers-by are considered when siting equipment | | | | | |
| 3 | There is a UPS system or backup generator in place that is tested within an appropriate timescale | | | | | |
| 4 | The location of power and telecommunications cables is protect from interference, interception or damage | | | | | |
| 5 | There is a well enforced and well communicated process for controlling how assets are removed from site and spot checks are carried out | | | | | |
| 6 | Policies and technical controls apply in securing equipment that are inadvertently left unattended. | | | | | |
| 7 | A clear desk and/or clear screen policy are well enforced in the organization | | | | | |

## 5. SYSTEM SECURITY

| NO | Questions | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| 1 | The SACCO develop software or systems in-house and there are policies mandating the implementation and assessment of security controls | | | | | |
| 2 | The SACCO specifies information security requirements during introduction, enhancement, or upgrade of systems. | | | | | |
| 3 | The SACCO applications that send information over public networks properly shield the information against fraud, contract dispute, unauthorized discloser and unauthorized modification | | | | | |
| 4 | There are controls in place for preventing information misrouting, incomplete transmission, unauthorized message alteration, unauthorized disclosure, replay attacks, or unauthorized message duplication. | | | | | |
| 5 | There are policies in place that mandate how and when software packages can be changed or modified | | | | | |
| 6 | Where software is developed in-house, proper utilization of secure development environment for all projects apply during the system development lifecycle | | | | | |
| 7 | There are requirements that externally developed code must be subjected to a security review and test before deployment | | | | | |

## 6. HUMAN RESOURCE SECURITY

| NO. | Questions | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| 1 | Background verification checks apply to all employment candidates and is approved by appropriate management authority | | | | | |
| 2 | All employees and contractors must sign confidentiality and nondisclosure agreements | | | | | |
| 3 | Managers engage in driving security within the SACCO and encourage all contractors and employees to apply security according to laid down policies and procedures. | | | | | |
| 4 | All employees and contractors undergo security awareness training regularly that is appropriate to their roles and function within the SACCO. | | | | | |
| 5 | There is an official disciplinary process through which the organization acts upon employees who breach information security. All employees are aware of the process. | | | | | |
| 6 | There is a documented process for changing employment duties or terminating employment that is communicated to the employees and/or contractors | | | | | |

## 7. ACCESS CONTROLS

| NO. | Questions | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| 1 | There is a well-documented and widely communicated access control policy in the organization. | | | | | |
| 2 | Controls exist for ensuring that users can only access network resources necessary for their duties. | | | | | |
| 3 | The SACCO has a formal user access registration process and a formal access assignment process to assign access rights for all users. | | | | | |
| 4 | Formal management processes and policies are in place for controlling the allocation of secret authentication. | | | | | |
| 5 | Processes exist for ensuring that user access rights are revoked upon termination of contractor employment, or adjusted when their roles change. | | | | | |
| 6 | Strict access control policy applies to restrict access to information and application system functions. | | | | | |
| 7 | Password systems are interactive and enforce complex passwords requirements | | | | | |

## 8. COMPLIANCE

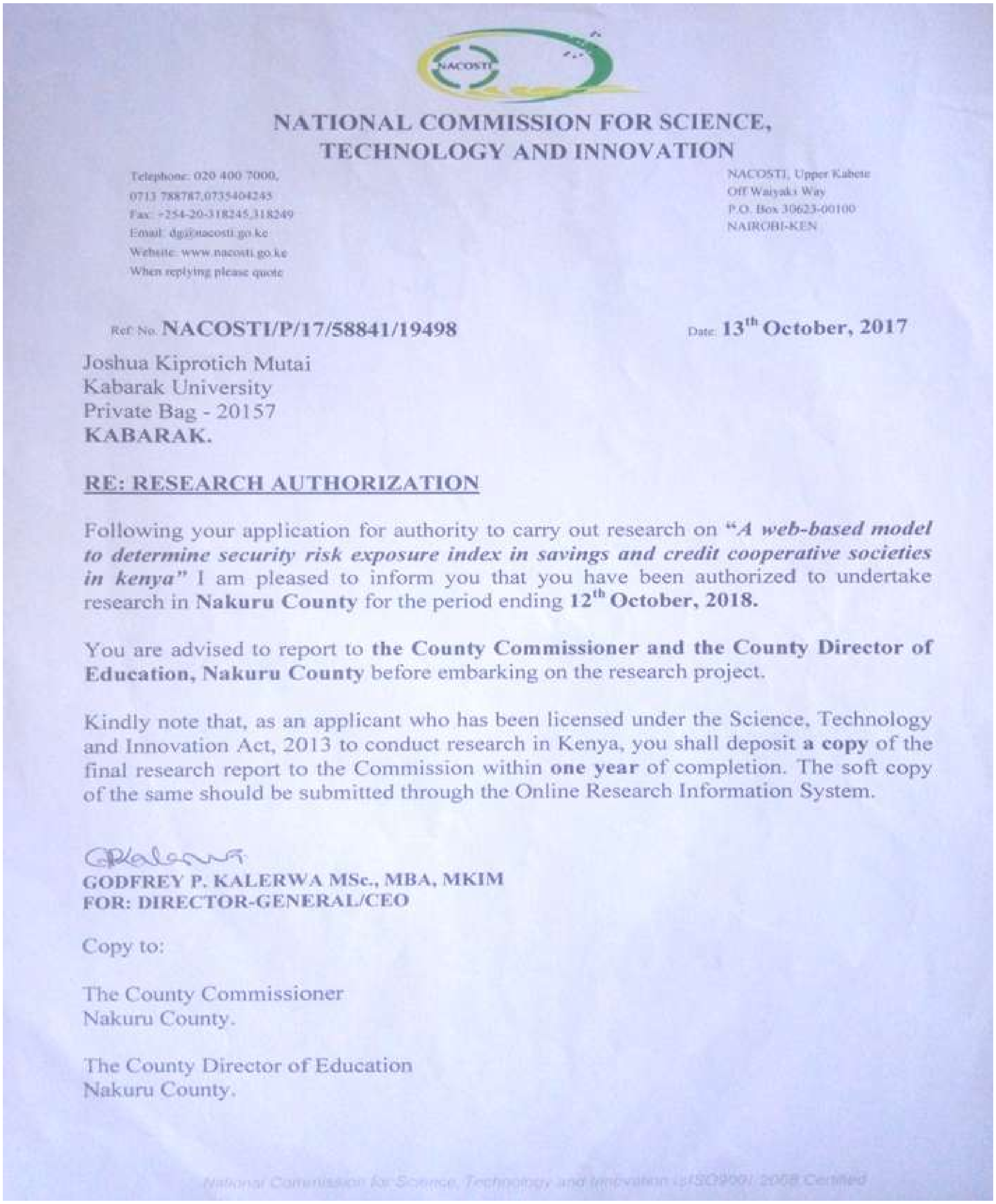
| NO. | Questions | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| 1 | Our SACCO has identified and documented all applicable contractual, legislative or regulatory requirements concerning security | | | | | |
| 2 | The SACCO maintains a record of all proprietary software products and intellectual property rights and monitor use of unlicensed software | | | | | |
| 3 | All the records within the SACCO are protected from loss, destruction, falsification and unauthorized access or release in conformity with contractual, regulatory, legislative and business requirements | | | | | |
| 4 | The SACCO protect personal data in strict compliance with relevant legislation | | | | | |
| 5 | The SACCO ensures that the implementation of security controls and information security is subject to regular independent reviews | | | | | |
| 6 | The SACCO managers under instruction to do policy and procedures' compliance reviews within their area of responsibility regularly | | | | | |
| 7 | The SACCO conducts technical compliance reviews of information systems regularly | | | | | |

## Appendix B: Licensed Deposit-taking SACCOs in Nakuru Central Business District

| No. | Name of the SACCO | Main Membership Type |
|---|---|---|
| 1 | 2NK SACCO Society ltd | Business |
| 2 | Afya SACCO Society ltd | Doctors |
| 3 | Boresha SACCO Society ltd | Teachers |
| 4 | Cosmopolitan SACCO Society ltd | Teachers |
| 5 | Harambee SACCO Society ltd | Workers |
| 6 | Metropolitan National SACCO Society ltd | Teachers |
| 7 | Mwalimu National SACCO Society ltd | Teachers |
| 8 | Stima SACCO Society ltd | Workers |
| 9 | Unaitas SACCO Society ltd | Farmers |
| 10 | Uni-County SACCO Society ltd | Workers |
| 11 | Vision Africa SACCO Society ltd | Business |

Source: (SASRA, 2015)

# Appendix C: NACOSTI Research Authorization



NATIONAL COMMISSION FOR SCIENCE,
TECHNOLOGY AND INNOVATION

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

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

Ref: No. **NACOSTI/P/17/58841/19498**

Date: **13th October, 2017**

Joshua Kiprotich Mutai
Kabarak University
Private Bag - 20157
**KABARAK.**

**RE: RESEARCH AUTHORIZATION**

Following your application for authority to carry out research on ***"A web-based model to determine security risk exposure index in savings and credit cooperative societies in kenya"*** I am pleased to inform you that you have been authorized to undertake research in **Nakuru County** for the period ending **12th October, 2018.**

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

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

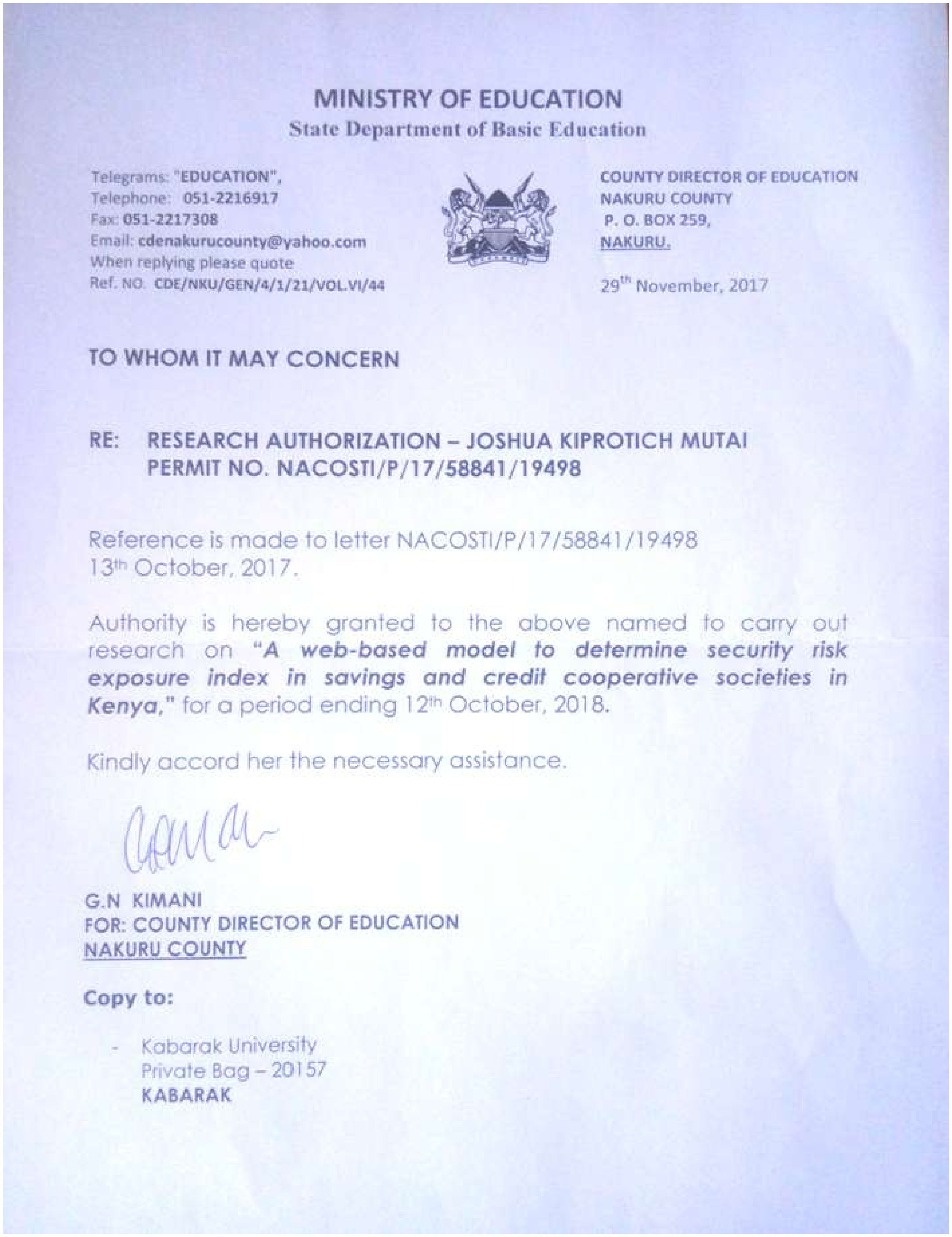
Copy to:

The County Commissioner
Nakuru County.

The County Director of Education
Nakuru County.

*National Commission for Science, Technology and Innovation is ISO9001: 2008 Certified*

## Appendix D: Ministry of Education Research Authorization



**MINISTRY OF EDUCATION**
**State Department of Basic Education**

Telegrams: "EDUCATION",
Telephone: 051-2216917
Fax: 051-2217308
Email: cdenakurucounty@yahoo.com
When replying please quote
Ref. NO. CDE/NKU/GEN/4/1/21/VOL.VI/44

COUNTY DIRECTOR OF EDUCATION
NAKURU COUNTY
P. O. BOX 259,
NAKURU.

29th November, 2017

**TO WHOM IT MAY CONCERN**

**RE: RESEARCH AUTHORIZATION – JOSHUA KIPROTICH MUTAI**
**PERMIT NO. NACOSTI/P/17/58841/19498**

Reference is made to letter NACOSTI/P/17/58841/19498
13th October, 2017.

Authority is hereby granted to the above named to carry out research on ***"A web-based model to determine security risk exposure index in savings and credit cooperative societies in Kenya,"*** for a period ending 12th October, 2018.

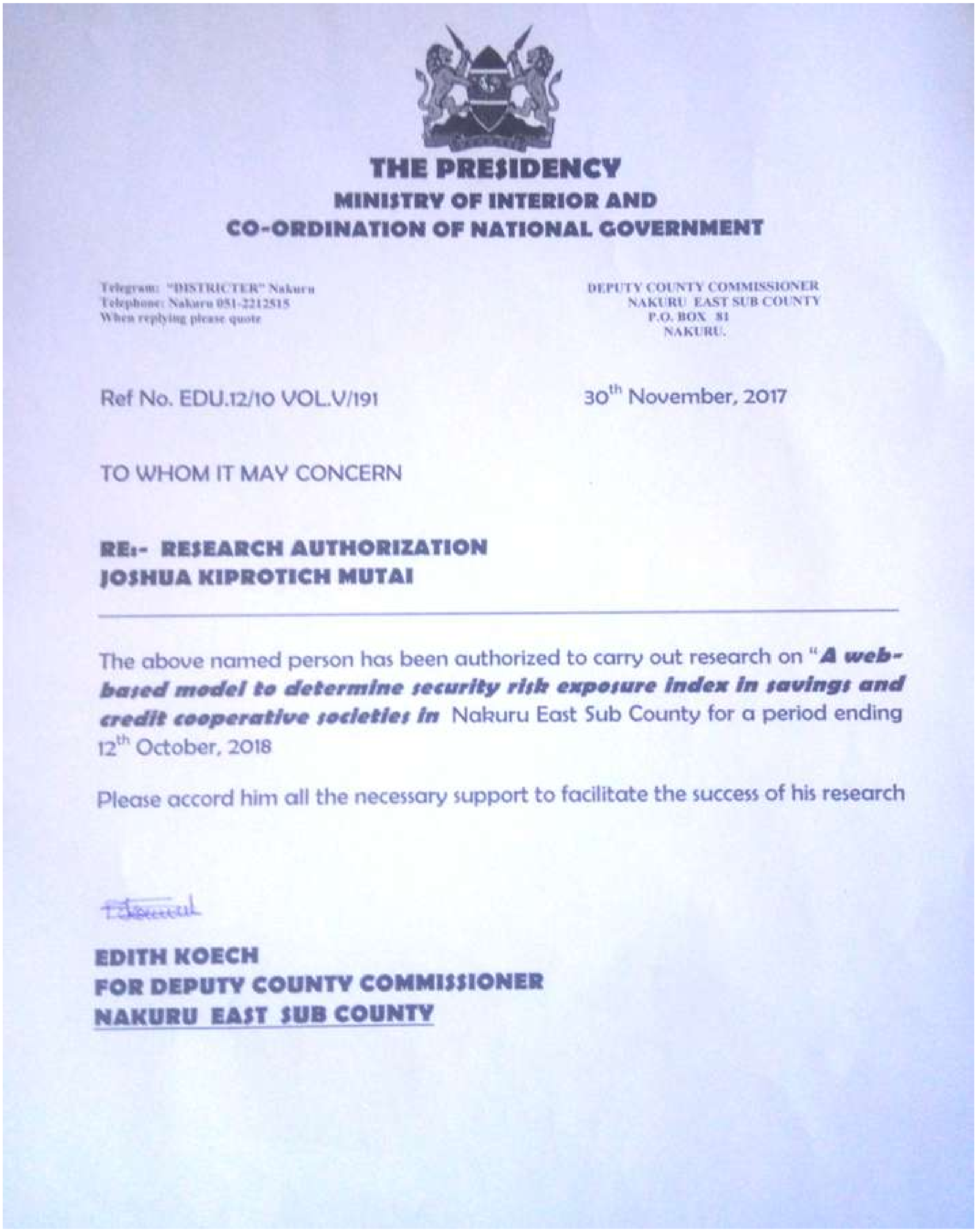
Kindly accord her the necessary assistance.

G.N KIMANI
FOR: COUNTY DIRECTOR OF EDUCATION
NAKURU COUNTY

**Copy to:**

- Kabarak University
  Private Bag – 20157
  KABARAK

# Appendix E: Ministry of Interior and Co-ordination on National Government Research Authorization



**THE PRESIDENCY**
**MINISTRY OF INTERIOR AND**
**CO-ORDINATION OF NATIONAL GOVERNMENT**

Telegram: "DISTRICTER" Nakuru
Telephone: Nakuru 051-2212515
When replying please quote

DEPUTY COUNTY COMMISSIONER
NAKURU EAST SUB COUNTY
P.O. BOX 81
NAKURU.

Ref No. EDU.12/10 VOL.V/191

30th November, 2017

TO WHOM IT MAY CONCERN

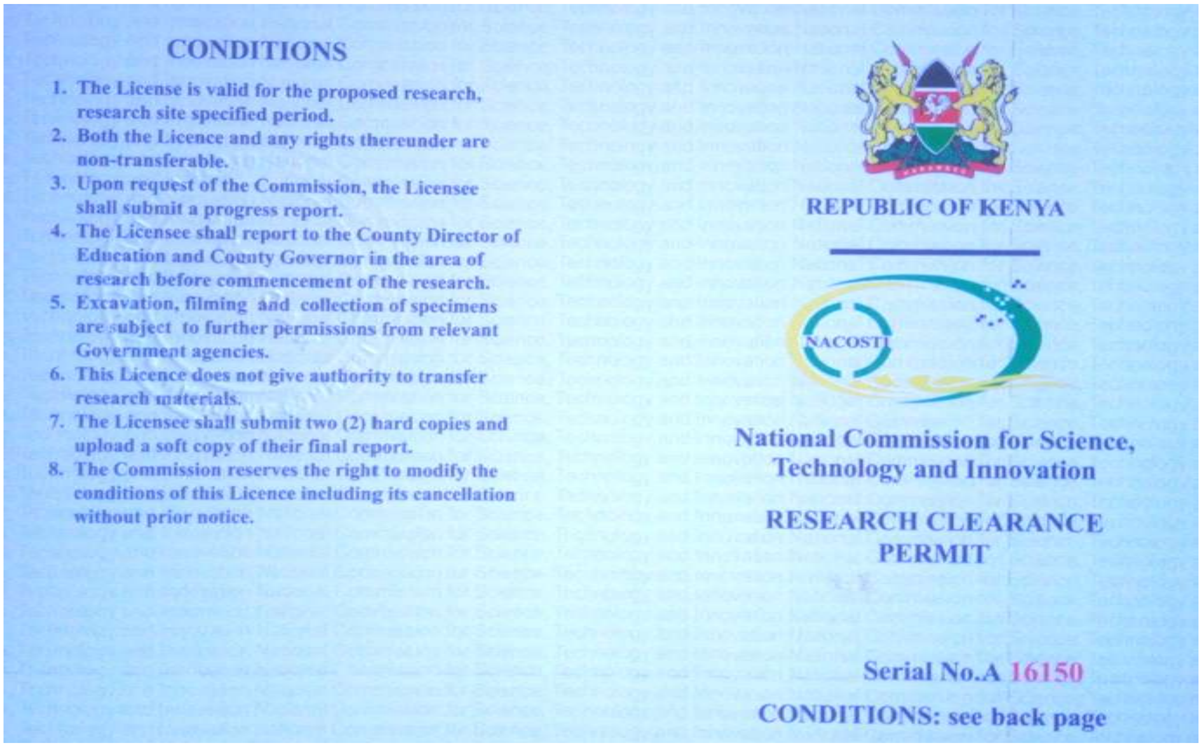
**RE:- RESEARCH AUTHORIZATION**
**JOSHUA KIPROTICH MUTAI**

The above named person has been authorized to carry out research on "***A web-based model to determine security risk exposure index in savings and credit cooperative societies in*** Nakuru East Sub County for a period ending 12th October, 2018

Please accord him all the necessary support to facilitate the success of his research

**EDITH KOECH**
**FOR DEPUTY COUNTY COMMISSIONER**
**NAKURU EAST SUB COUNTY**

# Appendix F: NACOSTI Research Clearance Permit



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

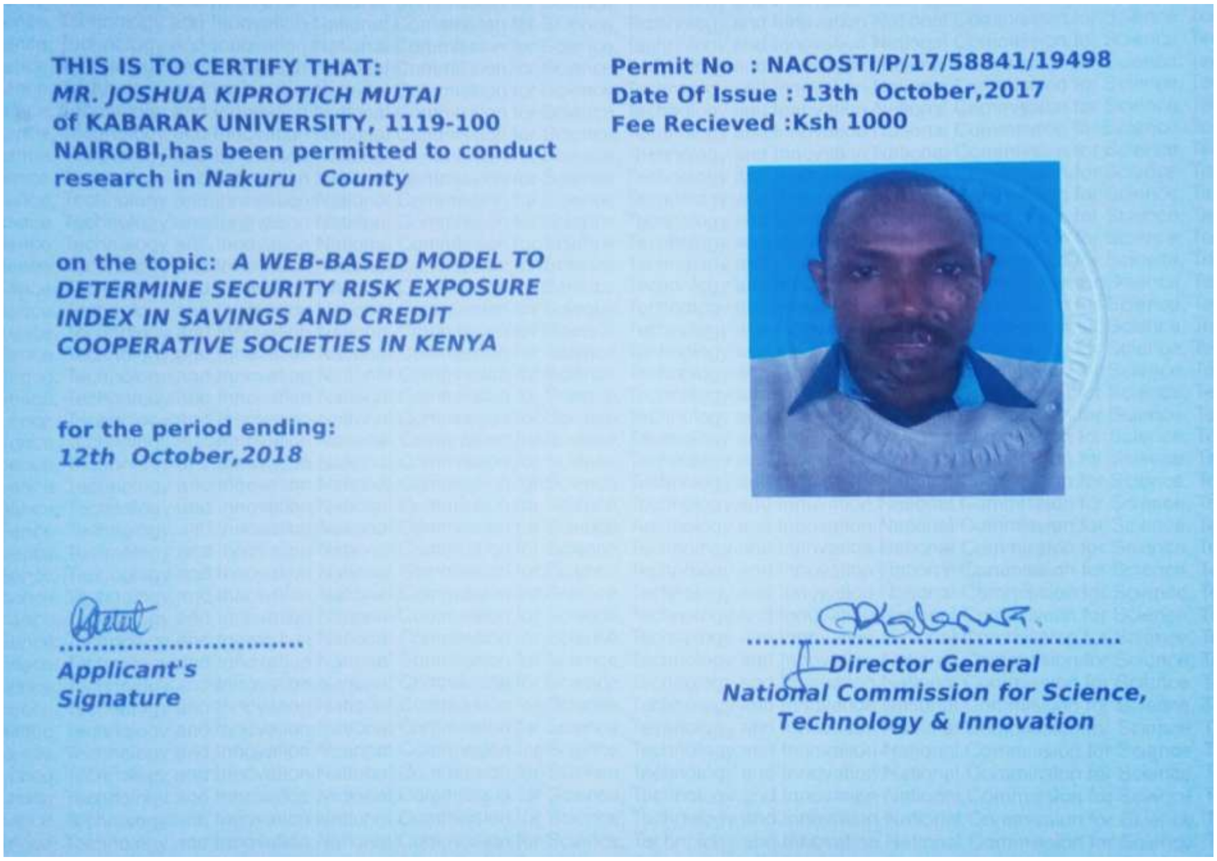
NACOSTI

National Commission for Science, Technology and Innovation

RESEARCH CLEARANCE PERMIT

Serial No.A 16150

CONDITIONS: see back page



THIS IS TO CERTIFY THAT:
*MR. JOSHUA KIPROTICH MUTAI*
of KABARAK UNIVERSITY, 1119-100
NAIROBI,has been permitted to conduct research in *Nakuru County*

on the topic: *A WEB-BASED MODEL TO DETERMINE SECURITY RISK EXPOSURE INDEX IN SAVINGS AND CREDIT COOPERATIVE SOCIETIES IN KENYA*

for the period ending:
*12th October,2018*

Permit No : NACOSTI/P/17/58841/19498
Date Of Issue : 13th October,2017
Fee Recieved :Ksh 1000

..............................
*Applicant's Signature*

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

# Appendix G: System Code

**UserRegistration** *******************************************************

```
<?php
session_start();
if(isset($_SESSION[‘usr_id’])) {
   header(“Location: index.php”);
}
include_once ‘dbconnect.php’;
//set validation error flag as false
$error = false;
//check if form is submitted
if (isset($_POST[‘signup’])) {
   $name = mysqli_real_escape_string($con, $_POST[‘name’]);
          $username = mysqli_real_escape_string($con, $_POST[‘username’]);
   $email = mysqli_real_escape_string($con, $_POST[‘email’]);
          $organization = mysqli_real_escape_string($con, $_POST[‘organization’]);
   $password = mysqli_real_escape_string($con, $_POST[‘password’]);
   $cpassword = mysqli_real_escape_string($con, $_POST[‘cpassword’]);
   //name can contain only alpha characters and space
   if (!preg_match(“/^[a-zA-Z ]+$/”,$name)) {
      $error = true;
      $name_error = “Name must contain only alphabets and space”;
   }
   if(!filter_var($email,FILTER_VALIDATE_EMAIL)) {
      $error = true;
      $email_error = “Please Enter Valid Email ID”;
   }
   if(strlen($password) < 6) {
      $error = true;
      $password_error = “Password must be minimum of 6 characters”;
   }
   if($password != $cpassword) {
        $error = true;
        $cpassword_error = “Password and Confirm Password doesn’t match”;
    }
    if (!$error) {
        if(mysqli_query($con, “INSERT INTO users(name,username,organization,email,password)
VALUES(“‘ . $name . “‘,’“ . $username . “‘,’“ . $organization . “‘, “‘ . $email . “‘, “‘ .
md5($password) . “‘)”)) {
            $successmsg = “Successfully Registered! <a href=‘login.php’>Login</a>“;
        } else {
            $errormsg = “Error in registering...Please try again later!”;
        }
    }
}
?>
<!DOCTYPE html>
<html>
<head>
<title>SREI | User Registration</title>
<meta content=“width=device-width, initial-scale=1.0” name=“viewport”>
<link rel=“stylesheet” href=“css/bootstrap.min.css” type=“text/css” />
</head>
<body>
<nav class=“navbar navbar-default” role=“navigation”>
<div class=“container-fluid”>
<!-- add header -->
<div class=“navbar-header”>
<button type=“button” class=“navbar-toggle” data-toggle=“collapse” data-target=“#navbar1”>
<span class=“icon-bar”></span>
<span class=“icon-bar”></span>
<span class=“icon-bar”></span>
</button>
<a class=“navbar-brand” href=“home.php”>SREI</a>
</div>
<!-- menu items -->
```

```
<div class=“collapse navbar-collapse” id=“navbar1”>
<ul class=“nav navbar-nav navbar-right”>
<li><a href=“index.php”>Login</a></li>
</ul>
</div>
        </div>
</nav>
<div class=“container”>
<div class=“row”>
<div class=“col-md-4 col-md-offset-4 well”>
<form role=“form” action=“<?php echo $_SERVER[‘PHP_SELF’]; ?>“ method=“post”
name=“signupform”>
<fieldset>
<legend>SREI | User Registration</legend>

<div class=“form-group”>
<label for=“name”>Name</label>
<input type=“text” name=“name” placeholder=“Enter Full Name” required value=“<?php if($error)
echo $name; ?>“ class=“form-control” />
<span class=“text-danger”><?php if (isset($name_error)) echo $name_error; ?></span>
</div>
        <div class=“form-group”>
<label for=“name”>UserName</label>
<input type=“text” name=“username” placeholder=“Enter prefered username” required value=“<?php
if($error) echo $username; ?>“ class=“form-control” />
<span class=“text-danger”><?php if (isset($username_error)) echo $username_error; ?></span>
</div>

                                        <div class=“form-group”>
<label for=“name”>Organization</label>
<input type=“text” name=“organization” placeholder=“Enter your organization “ required
value=“<?php if($error) echo $organization; ?>“ class=“form-control” />
<span class=“text-danger”><?php if (isset($org_error)) echo $org_error; ?></span>
</div>
```

```
<div class=“form-group”>
<label for=“name”>Email</label>
<input type=“text” name=“email” placeholder=“Email” required value=“<?php if($error) echo $email; ?>“ class=“form-control” />
<span class=“text-danger”><?php if (isset($email_error)) echo $email_error; ?></span>
</div>
<div class=“form-group”>
<label for=“name”>Password</label>
<input type=“password” name=“password” placeholder=“Password” required class=“form-control” />
<span class=“text-danger”><?php if (isset($password_error)) echo $password_error; ?></span>
</div>
<div class=“form-group”>
<label for=“name”>Confirm Password</label>
<input type=“password” name=“cpassword” placeholder=“Confirm Password” required class=“form-control” />
<span class=“text-danger”><?php if (isset($cpassword_error)) echo $cpassword_error; ?></span>
</div>
<div class=“form-group”>
<input type=“submit” name=“signup” value=“Register” class=“btn btn-primary” />
</div>
</fieldset>
</form>
<span class=“text-success”><?php if (isset($successmsg)) { echo $successmsg; } ?></span>
<span class=“text-danger”><?php if (isset($errormsg)) { echo $errormsg; } ?></span>
</div>
</div>
<div class=“row”>
<div class=“col-md-4 col-md-offset-4 text-center”>
<a href=“index.php”>Login Here</a>
</div>
</div>
</div>
<script src=“js/jquery-1.10.2.js”></script>
```

```
<script src="js/bootstrap.min.js"></script>
</body>
</html>
```

**Login** ****************************************************************

```
<?php
session_start();
if(isset($_SESSION['usr_id'])!="") {
   header("Location: index.php");
}
include_once 'dbconnect.php';
//check if form is submitted
if (isset($_POST['login'])) {
   $email = mysqli_real_escape_string($con, $_POST['emailorusername']);
            $password = mysqli_real_escape_string($con, $_POST['password']);
   $result = mysqli_query($con, "SELECT * FROM users WHERE (email ='" . $email. "' or username='" . $email. "') and password='" . md5($password) . "'");
   if ($row = mysqli_fetch_array($result)) {
      $_SESSION['usr_id'] = $row['id'];
      $_SESSION['usr_name'] = $row['name'];
      header("Location: home.php");
   } else {
      $errormsg = "Email/Password or Password is incorrect!";
   }
}
?>

<!DOCTYPE html>
<html>
<head>
<title>SREI | Login</title>
<meta content="width=device-width, initial-scale=1.0" name="viewport">
<link rel="stylesheet" href="css/bootstrap.min.css" type="text/css" />
            <link rel="stylesheet" href="css/sreistyle.css" type="text/css" />
```

```
        <link rel=“stylesheet” href=“css/questionnaire.css” type=“text/css” />
</head>
<body>
<nav class=“navbar navbar-default” role=“navigation”>
<div class=“container-fluid”>
<!-- add header -->
<div class=“navbar-header”>
<button type=“button” class=“navbar-toggle” data-toggle=“collapse” data-target=“#navbar1”>
<span class=“icon-bar”></span>
<span class=“icon-bar”></span>
<span class=“icon-bar”></span>
</button>
<a class=“navbar-brand” href=“home.php”>SREI</a>
</div>
<!-- menu items -->
<div class=“collapse navbar-collapse” id=“navbar1”>
<ul class=“nav navbar-nav navbar-right”>
                        <p id=“salutation”> Welcome to SREI Platform</p>
</ul>
</div>
</div>
</nav>
<div id=“welcomepage”>
<div class=“container”>
<div class=“row”>
<div class=“col-md-4 col-md-offset-4 well”>
<form role=“form” action=“<?php echo $_SERVER[‘PHP_SELF’]; ?>“ method=“post”
name=“loginform”>
<fieldset>
<legend>SREI System | Login</legend>
<div class=“form-group”>
<label for=“name”>Username or Email</label>
<input type=“text” name=“emailorusername” placeholder=“Your Username or Email” required
class=“form-control” />
```

```
</div>
<div class="form-group">
<label for="name">Password</label>
<input type="password" name="password" placeholder="Your Password" required class="form-control" />
</div>
<div class="form-group">
<input type="submit" name="login" value="Login" class="btn btn-primary" />
        <div id="login_register"><p>OR REGISTER HERE</p><a href="register.php" id="regicon">Register</a></div>
</div>
</fieldset>
</form>
<span class="text-danger"><?php if (isset($errormsg)) { echo $errormsg; } ?></span>
</div>
</div>
</div>
</div>
<div id="footer">
<p>Designed by Joshua Mutai for MSC. IT Security & Audit Project - KABARAK UNIVERSITY (2017)</p>
</div>
<script src="js/jquery-1.10.2.js"></script>
<script src="js/bootstrap.min.js"></script>
</body>
</html>
```

**RiskAssessment**************************************************

```
<?php

        include_once 'dbconnect.php';
        //mysql_select_db('testdb');

        //Retrieve questions from the database
        $sql = "SELECT questionid, question FROM systemquestions";
```

```
$result = mysqli_query($con, $sql);
$json = array();

if (mysqli_num_rows($result) > 0) {
// output data of each row
echo “<table class=‘responstable’>
    <tr id=‘tableheader’>
    <th>Id</th>
    <th>Question</th>
    <th>SD</th>
    <th>D</th>
    <th>N</th>
    <th>A</th>
    <th>SA</th>
    </tr>“;
while($row = mysqli_fetch_assoc($result)) {
    $test_data[]=$row;
    $json[‘responses’]=$test_data;
    $radioname = $row[‘questionid’];
    echo “<tr>“;
    echo “<td id=‘radiobutton’>“ . $row[‘questionid’] . “</td>“;
    echo “<td>“ . $row[‘question’] . “</td>“;

    for($i=1;$i<=5;$i++){
    echo “<td id=‘radiobuttons’><input type=‘radio’ name=‘$radioname’
    value=‘$i’/></td>“;
    }

    echo “</tr>“;
}
echo “</table>“;
echo “<p id=‘complete’>End of Assessment Questions</p>“;
```

```
            echo “<hr>“;
}else {
echo “<p id=‘complete’>No Questions in the database!</p>“;
echo json_encode($json);
}
if(isset($_POST[“submit_questionnair_btn”])){

//POSTING SCORES TO THE DATABASE

            $sql = “SELECT questionid, question FROM systemquestions”;
            $result = mysqli_query($con, $sql);

            while($row = mysqli_fetch_assoc($result)) {
                        $radioname = $row[‘questionid’];
                        @$user_id = $_SESSION[‘usr_id’];
                        @$userscore = $_POST[$radioname];

            if(@$_POST[‘submit_questionnair_btn’]){

                        $sql=“insert into assessment(userid,questionid,score)
                        values(‘$user_id’,’$radioname’,’$userscore’)”;
                        mysqli_query($con, $sql);
                                    }
                        }
            }
            ?>
<?php
include_once ‘dbconnect.php’;

//SREI COMPUTATION
            $user_id = $_SESSION[‘usr_id’];
```

```
        $sql = “SELECT 100-round(sum(score)/(COUNT(questionid)*5)*100,1)FROM
        assessment where assessmentdate >= CURDATE() and userid=$user_id”;
        $result = mysqli_query($con,$sql);
        $data = mysqli_fetch_array($result);
        echo “<span id=‘index’>TODAY’S ASSESSMENT RESULTS: </br></span>“;
        echo ‘<span>You are &nbsp<input type=“text” id=“take-input” class=“take-
        input”value=“‘.$data[0].’“ readonly/></span>‘;
        echo “<span id=‘indexs’>&nbsp% &nbsp Exposed</span>“;
        echo “<hr>“;
?>
```

**Recommendations** ***********************************************

```
<?php
session_set_cookie_params(0);
 session_start();
function fetch_data() {
    include_once ‘dbconnect.php’;


         $user_id = $_SESSION[‘usr_id’];
         $output = ‘‘;
    $sql = “SELECT a.questionid,c.category,b.score AS YourScore,a.recommendations FROM
systemquestions a INNER JOIN assessment b
              ON a.questionid=b.questionid INNER JOIN quizcategories c on
a.categoryid=c.categoryid WHERE b.userid=$user_id and b.score<a.thresholdscore
              ORDER BY a.questionid,c.category”;
    $result = mysqli_query($con, $sql);
    while($row = mysqli_fetch_array($result))
    {
    $output .= ‘<tr>
<td>‘.$row[“questionid”].’</td>
<td>‘.$row[“YourScore”].’</td>
<td>‘.$row[“recommendations”].’</td>

</tr>
‘;}
    return $output;
 }
 if(isset($_POST[“download_assessment_btn”]))
 {
    require_once(‘tcpdf/tcpdf.php’);
          ini_set(‘max_execution_time’, 10800);
          ini_set(‘pcre.backtrack_limit’, 30000000);
          $obj_pdf = new TCPDF(PDF_PAGE_ORIENTATION, PDF_UNIT, ‘LETTER’, true, 
‘UTF-8’, false);
    $obj_pdf->SetCreator(PDF_CREATOR);
    $obj_pdf->SetTitle(“SREI Recommendations”);
    $obj_pdf->SetHeaderData(‘‘, ‘‘, PDF_HEADER_TITLE, PDF_HEADER_STRING);
    $obj_pdf->setHeaderFont(Array(PDF_FONT_NAME_MAIN, ‘‘, PDF_FONT_SIZE_MAIN));
    $obj_pdf->setFooterFont(Array(PDF_FONT_NAME_DATA, ‘‘, PDF_FONT_SIZE_DATA));
    $obj_pdf->SetDefaultMonospacedFont(‘helvetica’);
    $obj_pdf->SetFooterMargin(PDF_MARGIN_FOOTER);
          $obj_pdf->SetMargins(PDF_MARGIN_LEFT, ‘5’, PDF_MARGIN_RIGHT,true);
    $obj_pdf->setPrintHeader(False);
    $obj_pdf->setPrintFooter(false);
    //$obj_pdf->SetAutoPageBreak(TRUE, 10);
    $obj_pdf->SetFont(‘helvetica’, ‘‘, 8);
    $obj_pdf->AddPage();
    $content = ‘‘;
    $content .= ‘
<h3 align=“center”>SREI SYSTEM | YOUR RECOMMENDATIONS</h3><br /><br />
<table border=“1” cellspacing=“0” cellpadding=“5”>
<tr>
<th width=“10%”>QUESTION</th>
<th width=“10%”>SCORE</th>
<th width=“75%”>RECOMMENDATIONS</th>
</tr>
‘;
    $content .= fetch_data();
    $content .= ‘</table>‘;
            $obj_pdf->writeHTML($content);
            //$obj_pdf->writeHTML($content, true, false, false, false, ‘‘);
    $obj_pdf->Output(‘Recommendations.pdf’, ‘I’);
}
?>
```