UNIVERSITY OF NAIROBI
SCHOOL OF COMPUTING AND INFORMATICS

IMPLEMENTATION FRAMEWORK FOR INFORMATION SYSTEMS POLICY FOR FRAUD CONTROL IN CREDIT UNIONS

By
Oronje Samuel Lubanga
P54/65722/2013

Supervisor:
Christopher A. Moturi

Research Project Report Submitted in Partial Fulfillment of the Requirements of the Master of Science in Information Technology Management

January 2015

DECLARATION

This project is my original work and to the best of my knowledge this research work has not been submitted for any other award in any University

Oronje Samuel Lubanga: …………………… Date: …………………………….
(P54/65722/2013)

This project report has been submitted in partial fulfillment of the requirement of the Master of Science in Information Technology Management of the University of Nairobi with my approval as the University supervisor.

Christopher A. Moturi: é é é é é é é é é é é .. Date: é é é é é é é é é é é ..
Deputy Director,
School of Computing and Informatics.

ACKNOWLEDGEMENT

It is with great gratitude to God who enabled me both health-wise and spiritually through to the success of this study. The Deputy Director Mr. Moturi of School of Computing and Informatics of University of Nairobi played a very important role and is highly acknowledged as the Supervisor of this study. I do also thank the Chairman of the assessment panel Dr. Abade for the guidance and direction through the various levels of preparation. It would not be possible to reach this far without the entire administration and management of the University of Nairobi which provided the right facilities and granted me an opportunity in the School. I am also grateful to my family, friends and all those who supported me in countless ways. Your assistance will always be remembered.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ACRONYMS

ATM	- Automated Teller Machine
DT	- Deposit Taking
IS	- Information Systems
IT	- Information Technology
ICT	- Information and Communication Technology
Ksh.	- Kenyan Shillings
SACCO	- Savings and Credit Co-operative Society
SACCOs	- Savings and Credit Co-operative Societies
SASRA	- SACCO Societies Regulatory Authority

DEFINITION OF TERMS

Adoption: This is a process that begins with awareness of the technology and progresses through assessment, acceptance to appropriate and effective usage.

Credit Unions: A Credit Union is member owned financial cooperatives that provide savings, credit and other financial services to their members which is based on a common bond, a linkage shared by savers and borrowers who belong to a specific community, organization, religion or place of employment.

Framework: this is a real or conceptual structure intended to serve as a support or guide for the building of something that expands the structure into something useful and may be for a set of functions within a given system and how they interrelate to have a resultant standardize desired performance.

Information Systems: This is a variety of disciplines such as the analysis and design of systems, computer networking, information security, database management and decision support systems which aims to support operations, management and decision making.

Policy: A policy is a statement of intent and is implemented as a procedure or protocol to guide decisions by considering the relative merits of a number of factors to achieve rational outcomes.

ABSTRACT

A gap exists of implementing IS policy making it difficult to achieve desired impact of securing Systems. The resultant problem is fraud which prevails in organizations even though there are documented policies. Four objectives which guided this study included: to establish the level of implementation of IS policy framework, to determine the extent of fraud occurrence on Information Systems (IS), to determine the potential fraud level exposure and to identify implementation framework for IS policy. The research adopted a descriptive survey design. The targeted population consisted 43 licensed deposit taking Credit Unions within Nairobi Metropolitan Region in Kenya (East Africa). A total of 140 questionnaires were distributed of which 125 were returned and validated. Results demonstrated that low level of implementation of policies lead to high fraud rate and higher chances of future occurrence of fraud. The enforcement level of the policies was also realized to be directly proportional to the impact level. This indicated that the documented policies within the organizations required an implementation framework. Presence of IS policies in isolation as studied was not sufficient to control fraud in organizations. This study concluded with demonstrating use of the 6x6 Zachmanôs framework to implement IS policies.

CHAPTER ONE: INTRODUCTION

1.1 Background of the Study

There existed a challenge to implement IS policies as mentioned by Askarov & Chong (2012). This challenge arose given that IS policy to be implemented on information frequently changed in systems that handled confidential data. Attackers could easily learn information in accordance with such a policy and invade the system. Such scenario resulted to a gap of implementation of IS policies since as new users kept joining the system the old ones left and also sensitivity of data changed over time. As the sensitivity of data changed, the policy had to be re-defined to ensure that it was carefully implemented by all who accessed the system to restrain risk of exposure to threat issues such as fraud. It would however, be impossible to always keep at pace in the rapid changing of policies to handle the risks which would result rather than to have a framework of IS policies in place which would sustain implementation of existing policies.

This study aimed to select a framework which would aid in implementing IS policies. The purpose was to have documented policies fitted in a selected framework to produce the desired impact. Fraud was handled in this case as the problem which ought to be controlled by the IS framework within Credit Unions. SACCOs; which refer to Credit Unions in Kenya had a great financial potential as indicated by statistics from SASRA (2012). In the report the total sectorôs assets stood at Kshs. 293 billion which was an increase of 17.7% from Kshs. 249 billion in the previous year. Its total membership had also grown by 15% from 2.6 million members in 2011 to 3 million in December 2012. The sector recorded to have high deposits which stood at Kshs.213 billion which posted an increase of 18.4 % from Kshs. 179.9 billion in 2011. These huge numbers of membership, deposits and asset value pointed out that Credit Unions were important contributors to the financial sector.

Fraud was pointed out as a threat subjecting the huge finances, assets and members deposits investments to loss as documented in SASRA (2011) report. The report emphasized an increase in incidences of fraud as ICT deployment expands among the Deposit Taking Sacco societies. The finding by Lin, Song & Sun (2011) which indicated that corporate fraud had a real impact on corporate outcomes by affecting the external financing cost and internal cash holdings also indicated that fraud is a threat to the growth of this sector and requires appropriate measures to counter.

1.2 Problem Statement

Credit Unions deploy IS to manage an array of financial products including demand savings account, ATM and custodial services through interlinking functions originating from a centralized database as documented by SASRA (2012). Employees and other authorized stakeholders interact with various functionalities of the IS during their daily assignments. All these interactions initiate transactions processing through the IS. There also exists sensitive databases which contain tables with valuable monetary records under store which require proper security. Policies would be formulated to define how to access and handle such processes with integrity to safe guard such systems.

Fraud is a problem which prevails within Credit Unions even though there is proof of existing documented policies. It was reported by Morgan (2014) that criminals use techniques that were continually more sophisticated and constantly evolving challenging financial professionals as they are tasked with anticipating possible fraud attempts on their organizations. This results to financial loss to individuals who access IS either directly or indirectly. It is therefore, not sufficient enough to have documented policies but rather have a way in which they would be effectively implemented through a selected IS policy framework to have the desired impact in mitigating fraud. It was noted in the policy paper done by Waema & Ndungû (2012) that in Kenya there was a draft ICT policy on the website of the Ministry of Information and Communications (MoIC) since February, 2011 for comment. This is a likely indication that the ICT policies required a proper framework to aid in their implementation otherwise the draft could not be open for comments.

1.3 Objectives

The study was guided by the following objectives:

1. To establish the level of implementation of IS policy framework by the Credit Unions.
2. To determine the extent of fraud occurrence on IS within the Credit Unions.
3. To determine the potential fraud level exposure to the IS within the Credit Unions.
4. To identify and apply a framework for implementation of IS policy for the Credit Unions.

1.4 Research Questions

There was necessity to implement an IS policy framework with the rapid growth of Credit Unions. This would aid in alleviation of fraud. The objectives which aided in development of such a framework were addressed by the following questions:

1. What is the level of implementation of IS policy framework elements in the Credit Unions?
2. What is the extend of fraud occurrences associated to IS has been detected in the Credit Unions?
3. What is the level of potential fraud which may occur in the IS within the Credit Unions?
4. How can a suitable policy framework be identified and applied to implement IS policy in Credit Unions?

1.4 Significance of the Study

This study will aid in the implementation of policies and aid in controlling fraud within Credit Unions. This would yield a positive impact in ensuring that the Information Systems are secure.

CHAPTER TWO: LITERATURE REVIEW

2.1 The SACCO Sector

The 2013 Statistical report indicated that there were 57,000 Credit Unions in 103 Countries on 6 Continents as documented by World Council of Credit Unions (2014). The Unions contributed 1.4 Trillion United States Dollars (USD) through Savings and Shares and had a total worth of 1.7 Trillion USD of Asset Value. 6,000 of these were located in Kenya contributing 2.659 and 4.466 Billion USD in Savings and Shares and Asset value respectively. SASRA (2012) report indicated that SACCOs have great financial contribution to the economy. Based on their asset base, three categories of SACCOs exist: large SACCOs which have assets of over KSh. 4 billion, a category with only 10; medium SACCOs which have assets between KSh.1 billion and KSh.4 billion, with 41 in this category; small SACCOs, which have assets less than KSh. 1 billion and represent the majority with 73 DT SACCOs. DT SACCOs are spread across the counties and can be further categorized from the sector in which the members are derived: Teacher based SACCOs (45), Government based (41), Farmers based (73), Private (24), and Community based (32). The total SACCOs population in Kenya is 215.

It was also noted from SASRA (2013) report that the total number of registered and non-registered Credit Unions was more than 6,000. From this total, 1,995 were active with only 215 falling under the D.T category. An important role played by SACCOs of enhancing high level of savings for investment as visualized in Vision 2030 was also cited. A record total of 48.55% of the National Savings were contributed by this Sector. The Kenya Economic report (2013) also confirmed that SACCOs play a critical role in the development process of the Vision 2030. This was due to the high level of savings required to finance investment needs.

2.2 Existing Frameworks

Several frameworks were studied with an aim to single out one for the purpose of applying to the Credit Unions. The desired blue print of the framework was to be easy to use and also capture all levels of operation and interaction with the IS such that the relevant policies can be clearly defined. The frameworks covered included: Zachman, COBIT, TOGAF, ISO27002 framework, DODAF framework and ITIL framework.

2.2.1 Zachman Framework

This is an IS Architecture framework which was introduced by Zachman, Radwan & Aarabi (2011). It is depicted as a 6x6 matrix which consists of two independent aspects namely: rows and columns. Rows represent six different audiences perspective from which a business or an enterprise can be perceived. The audience perspectives include: Owner, Designer Builder, bounded by the Scoping perspective, and the Implementation perspective. Columns represent various communication interrogatives which are functional to each view of the business or an enterprise. The interrogative expressions include: Data (What), Function (How), Network (Where), People (Who), Time (When) and Motivation (Why). The column generalizes information of a give enterprise, organization or set of guidelines. Intersection between the audience perspectives and interrogatives are represented by cells which provide classifications. The resultant matrix describes an enterprise wholesomely. This framework is an ontology implying it consists essential sets of components for explicit expression of an enterprise, a department, profession and even policies. The independence and holistic examination of the enterprise makes it differed from other architectural frameworks. The framework also is neutral in methodology, process, and technology, and considers the breadth of scope for the enterprise. The Unite States Department of Veterans Affairs used Zachmanœs Framework to define all functions related to each business process and identity of associated data elements. The framework was used to identify duplication of function and inconsistency in data definitions. The aim was to resolve any duplicating implementations of the same business function. Industrial products such as Buildings, Airplanes, Locomotives and Computers have also been developed using this architectural framework. Three major weaknesses of the framework include: lack of methodology covering all the aspects of the framework, a lack absence of repository storing the framework in accordance with the integrity rules and lack of a popular modeling details for all of the frameworkœs columns.

2.2.2 COBIT Framework

The practicability of COBIT framework in developing control objective has been shown through a model proposed by Zhang & Le (2013). This is an evaluation framework created by the IS Audit and Control Foundation (ISACF) in 1996. The widely used edition is COBIT 4.1 which was released in 2005 and revised in 2007. COBIT 5 is the latest which is developed through consolidation and integration of the element in COBIT 4.1. COBIT framework seeks to make IT controlled. This is attained by concentrating on information required to support the business objectives and requirements. Resultant information is a combination of application of IT-related resources and IT processes. Three components are considered namely: Information criteria, IT resources and IT processes. The elements in Information criteria include: Effectiveness, Efficiency, Confidentiality, Integrity, Availability, Compliance and Reliability. IT resources comprise the following: People, Applications, Technology, Facilities and Data. IT processes provides three main dimensions of COBITòs conceptual framework.

There exists a process description and a number of control objectives for each of the IT process. The generic IT processes are further classified into main domains. There are two-character domains which are used to identify control objectives together with a process number and also a control objective number. The domain reference attributes used include: PO: Plan and Organize, AI: Acquire and Implement, DS: Deliver and Support and ME: Monitor and Evaluate. COBIT 4.1 covers 222 control objectives which result from 34 high level processes. The resultant structure is a hierarchical presentation of IT activities from the highest domain level to IT processes and to the lowest level of IT activities. COBIT was designed to aid in management. IT professionals and auditors can be able to bridge the gap between business control models and IT control models. The element of risk control and investment can be managed. It is possible to use the guidelines provided for IT governance. The framework however has three weaknesses which include: being a non-pure technology standard for IT management since it required specific practices and standards covering discrete areas to be mapped up to the framework so that it can provide a hierarchy of guidance materials. Secondly, its complicated concepts and structure and finally lack of implementation guidance and proven benefits; whereby the generic nature COBIT creates great difficulty for organizations to understand and use it.

2.2.3 TOGAF Framework

TOGAF (The Open Group Architecture) framework presented by the Open Group (2014) was originally designed to support Technology Architecture. Developments have however taken course over the years making the framework a method for enterprise architecture. This framework enables IT users make design, evaluation, and building of the right architecture for their organization. It makes possible to reduce costs of planning, designing, and implementation of architectures based on open systems solutions. TOGAF Architecture Development Method (ADM) defines business needs and is used to develop an architecture using assets available to a particular organization. ADM is also an industry standard method, which is neutral towards tools and technologies. Products and other IT related elements including policies can be developed as long as they are recognized by any enterprise framework.

The benefits of TOGAF include: good governance in the level of transparency, accountability, and informed delegation of authority. Controlled risk management is possible. Existing asset base can be protected through maximizing re-use of existing architectural components, proactive control, monitoring, and management mechanisms. Processes, concept, and component can also be re-used across an enterpriseôs business units.
It is possible to add value to domains such as policy implementation in the measuring, evaluation, and feedback, increased visibility provided by the framework supports internal processes and external parties' requirements. However, TOGAF exposes weakness in that it is not independent but relays on what other frameworks have. It only provides a ADM that can be adapted. Also a number of enterprise architecture frameworks already exist which are widely recognized and preferred disadvantaging use of such a framework.

2.2.4 ISO 27002 Framework

The framework as described in the ISO (2013) documentation has two parts: the Introductory and the Standard. Introductory part contains three sections namely the Framework, Acceptable Use of Information Technology Resources and Information Security Definition & Terms. The Standard on the other hand contains twelve sections which include: Risk assessment, Security policy, Organization of information security, Asset management, Human resources security, Physical and environmental security, Communications and operations management, Access control, development and maintenance, Information security incident management, anticipating and responding appropriately to information security breaches Business continuity management. Each section contains information security controls with outlined specific objectives. The information security controls are generally regarded as best practice means of achieving the objectives. For each of the controls, implementation guidance is also provided.

2.2.5 DODAF Framework

Inception of DoDAF was in 1990 and was named ñCommand, Control, Communications, Computers, and Intelligenceò, (C4ISR). Interoperability is one of the key features the framework uses. A ñViewò model is used that comprise a high level ñAll Viewò that brings together three sets of views namely: operational, systems, and technical. These are used to define a product set. There exist 29 architectural products which are defined in detail relating to each view. The framework aids in visualizing and understanding architectural complexities using tables, text, and graphics. Cameron & McMillan (2013). However, DODAF does not distinguish views and viewpoints, which significantly complicated their description. As viewpoints, the DODAFôs definitions are incomplete. Stakeholders and concerns are not identified. This makes it difficult for the users to understand the reason why they were modeling, and when they process is complete.

2.2.6 ITIL Framework

Brooks (2012) presents ITIL framework for use as a basis of best practice guidance for IT service management, publications and associated lifecycle phases. The components entailed include: Service Strategy, Service Design, Service Transition, Service Operation and Continual Service Improvement. It provides a framework for the governance of IT, management and control of IT services. It focused on continual measurement and improvement of the quality of IT service delivered, from both a business and a customer perspective. Its benefits include: increased user and customer satisfaction with IT services, improved service availability, directly leading to increased business profits and revenue, financial savings, improved resource management and usage, improved time for marketing new products and services, enhanced decision making and reduced risk.

2.3 Fraud Concerns in Credit Unions

Credit Unions are reported to have problems of corruption and mismanagement. These revolve about issues including: gross mismanagement by officials, theft of cooperative resources, split of viable cooperatives into smaller ineffectual units, failure of employers to surrender membersô deposits to the cooperatives, failure to hold elections; nepotism in hiring and dismissal of staff, refusal of management committee members vacate after members voted for this dismissal, conflict of interest among cooperative officials, endless litigations, unauthorized cooperative investments as noted by Wanyama (2009). However, this study focused on fraud as a challenge within the Credit Unions.

It was noted by Lin, Song & Sun (2011) that the nature of corporate fraud differs in different surveys, arguments, and media coverage, yet corporate fraud pervasively exists and results to negative consequences. This is a vice both locally and internationally where Credit Unions were witnessed to have lost billions of shillings through fraud.   Warfield (2013) denotes that there is no organization which is able to completely stop fraud from happening. However, the survey indicates that a number of these organizations had large fraud occurrence that had not been discovered by their internal controls. It has been recognized in previous surveys of fraud that it was only when a fraudsterὂs routine is affected that many internal frauds came to light. Credit Unions are prone to such fraud occurrences where unsuspecting authorities are hit without their knowledge.

Fraud is a global concern which is encroached within Credit Unions. Statistics from the United States Department of the Treasury Financial Crimes Enforcement Network Advisory (2010) highlights a financial institutionὂs loan officer who deposited or withdrew large amounts of cash or large dollar checks in a manner inconsistent with his income or duties at the institution. The loan officer also would co-endorse checks for large amounts and depositing them into business or personal accounts, possibly at another financial institution.

Findings from Morgan (2013) points out that sixty-one percent of organizations experienced attempted or actual payments fraud in 2012. Sixty-seven percent of organizations with annual revenues over one billion United States (US) dollars were victims of payments fraud compared to half of those with annual revenues fewer than one billion US dollars.   From such reports, it clearly implied that unless an amicable solution was arrived at on how to mitigate fraud, it would be impossible to salvage Credit Unions from collapsing. Credit Unions which were also referred to as Co-operatives by Munkner (2013) had international guidelines which supported a good environment for their development. Fraud on the contrary is not a supportive environment which therefore ought to be controlled.

2.4 Conceptual Framework

The study was guided by the conceptual framework as shown in figure 1.

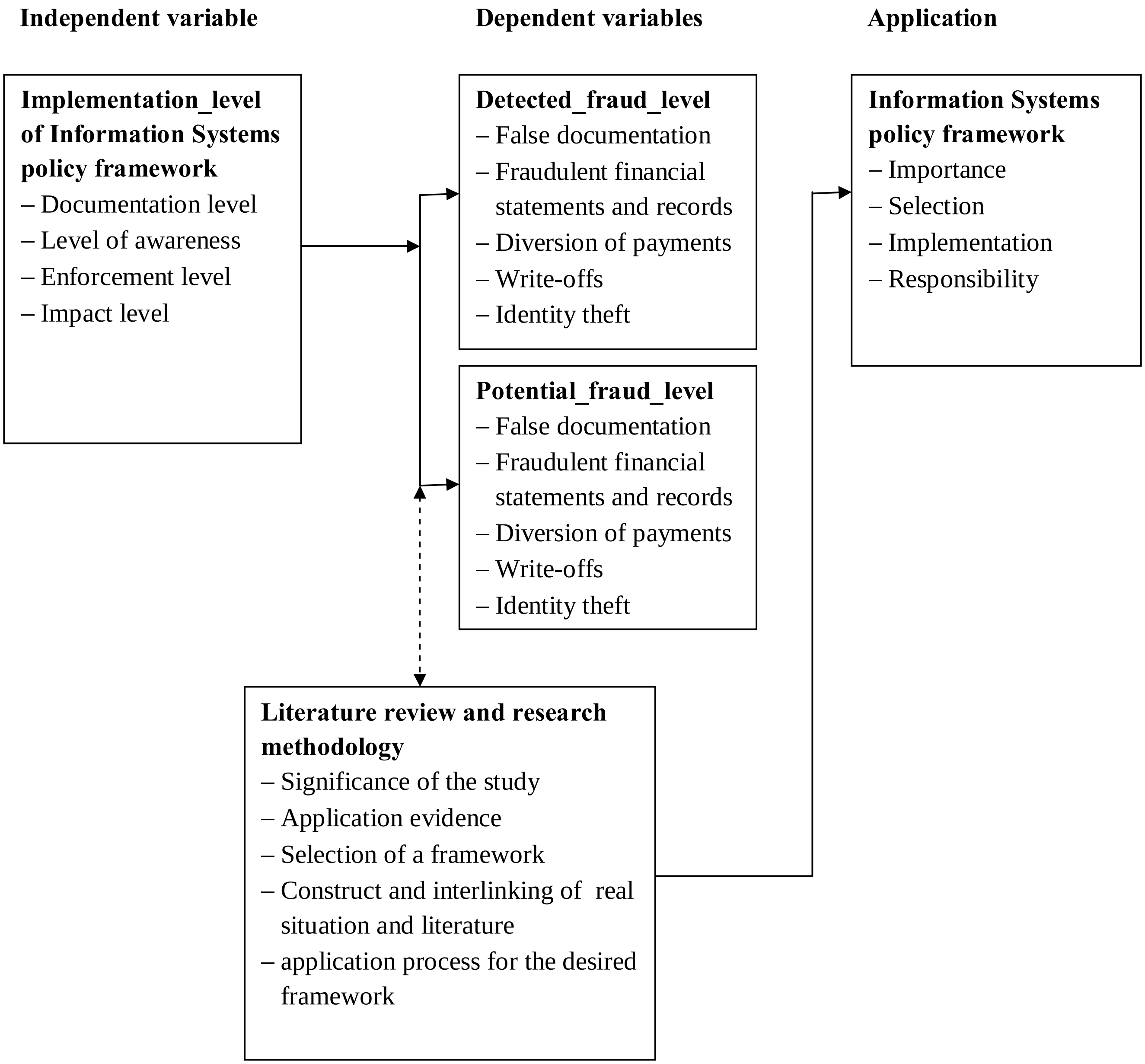
Independent variable
Dependent variables
Application
Implementation_level of Information Systems policy framework
– Documentation level
– Level of awareness
– Enforcement level
– Impact level
Detected_fraud_level
– False documentation
– Fraudulent financial statements and records
– Diversion of payments
– Write-offs
– Identity theft
Potential_fraud_level
– False documentation
– Fraudulent financial statements and records
– Diversion of payments
– Write-offs
– Identity theft
Information Systems policy framework
– Importance
– Selection
– Implementation
– Responsibility
Literature review and research methodology
– Significance of the study
– Application evidence
– Selection of a framework
– Construct and interlinking of real situation and literature
– application process for the desired framework

Figure 1: Conceptual framework **Source:** Author

Implementation level of IS policy framework was considered as an independent variable while the fraud levels and potential fraud channels were dependent variables. Literature review validated significance of in solving the problem and provided a set of frameworks for comparison and choice. Through the researchôs methodology, it was possible to conclude with a suitable framework of use to implement IS policies within the Credit Unions.

CHAPTER THREE: RESEARCH METHODOLOGY

3.1 Research Design

The research adopted descriptive survey design. A survey of Credit Unions within Nairobi Metropolitan Region was done through administering questionnaires. The region comprised four counties namely: Nairobi, Kiambu, Machakos and Kajiado. This research design was justified since it depended on the feedback of notable levels describing how fraud was evident in the Credit Unions. The level of implementation of IS policy framework was also realized making it possible to contribute to the findings. This was best achieved by presenting a set of common questions to all the Credit Unions. Field visit surveys facilitated studying of the respondents through observations. Survey of Nairobi Metropolitan Region provided a reasonable perspective of Credit Unions which can be translated both countrywide basing on the highest number of large Credit Unions located there as indicated in the next section.

3.2 Study Population

The target population consisted of licensed deposit taking Credit Unions within Nairobi Metropolitan Region. The population size consisted 43 licensed deposit taking Credit Unions enclosed within targeted region. Five respondents preferably from five different departments in each of these institutions gave a total population size of 215. The multiple of five was used basing assumption that all the Credit Unions considered had at least an equivalent number of departments to this.

There were 124 licensed deposit taking Credit Unions in 47 counties in Kenya from the total population of 215, as reported by SASRA (2012). 43 of these were considered since they were enclosed within the targeted region. This was an appropriate population size to base use since it represented all categories. In reference to assets value, Nairobi Metropolitan Region had 80% of the large Credit Unions which were valued at Ksh. 4 billion and above. It also included 60% of medium level which were valued between Ksh. 1 to Ksh. 4 billion and 26% of small Credit Unions, which were valued at less than Ksh. 1billion.

3.3 Sample Size Selection and Sampling Procedure

Taro Yamane formula was used to determine this sample size as follows:

$$n= \frac{N}{1+N*(e)^2}$$

Where:

n - The sample size,

N - The population size and

e - The acceptable sampling error (margin of error is 5 %)

Basing on a population size of 230 employees, the sample size was arrived at as follows:

$$n= \frac{215}{1+215*(0.05)^2}$$

$$=140$$

This sample size denoted the exact number of questionnaires issued to the respondents. Convenient sampling design was used where an individual would volunteer to participate as a respondent. The participants however, were required to have interacted with an IS or have knowledge about it within their organization. This gave a likelihood of getting adequate results from the respondents. Results gathered from administering questionnaires to the sample size population were assumed to represent matching view as the study population.

3.4 Data Collection Tools and Procedures

Data collection tools used included questionnaires, interviews and observations. Collection exercise was done for a period of two months. This was dependent on the speed at which the respondents provided their feedback. The process was initiated by phone calls, emails and field visits to forward transmittal letter to the respondents. 140 questionnaires were administered and were structured such that the respondents remained anonymous. Sample of a structured questionnaire is under appendix i. Semi-structured interviews were conducted in which the respondents were required to participate at will. From findings of surveys and interviews, it was possible to assess the level of fraud. Telephone conversations, email correspondences and field visits were used to initiate the interview sessions and also for follow-up purposes until adequate feedback was realized from the respondents. Observations were also done during field visits.

3.5 Validity of Data Collection Tools and Procedures

The questionnaire proved to be a valid and reliable instrument as Polikandrioti, Goudevenos, Michalis, Nikolaou, Dilanas, Olympios, Votteas & Elisaf (2011) concluded in their research. This resulted from 702 patients sampled from which a high repeatability of all sub-scales of questionnaire was identified through intra-class correlation coefficient (ICC). This indicated that data collected through structured questionnaires was considered valid. Interviews and observations were also valid and justified tools to use since they provided primary data from the field. It was possible to interact with the respondents who were directed on how to complete the questionnaires through interviews. An observation was done to confirm that the questionnaire was completed as required.

3.6 Data Processing and Analysis Method

Statistical Package for the Social Sciences (SPSS) version 22.0 software was used for data analysis. Scatter plots, correlation tables and charts were used to present data. Microsoft excel was also used to record all the data from the respondents. Correlations between three variables namely; Implementation_level of IS policy framework, Detected_fraud_level and Potential_ fraud_level were examined. A summary of data collected related to the conceptual framework was recorded as shown in appendix iii.

Table 3.1 Operations definition of variables

	Research Objectives	Variables	Indicators	Measure	Tools of analysis	Types of tools
1.	To establish the level of implementation of IS policy framework by the Credit Unions	Implementation_level of IS policy framework	– Documentation level – Level of awareness – Enforcement level – Impact level	Likert scale	Quantitative	Percentage and frequencies
2.	To determine the extent of fraud occurrences on IS within the Credit Unions.	Detected_ fraud_level	– False documentation – Fraudulent financial statements and records – Diversion of payments – Write-offs – Identity theft	Likert scale	Quantitative	Percentage and frequencies
3.	To determine the potential fraud level exposure to the IS within the Credit Unions.	Potential_ fraud_level	– False documentation – Fraudulent financial statements and records – Diversion of payments – Write-offs – Identity theft	Likert scale	Quantitative	Percentage and frequencies
4.	To apply a framework of IS policy for the Credit Unions.	IS policy framework	– Importance – Selection – Implementation – Responsibility	Likert scale	Qualitative	Percentage and frequencies

3.7 Limitation of Methodology and how they were Overcame

The descriptive survey design approach used made the outcome of this study to be biased to opinions of a few individuals who might not have been conversant with actual issues as required. This was overcome by structuring questionnaires from the elements of the conceptual framework. Population and sampling design was limited to licensed deposit taking Credit Unions within Nairobi Metropolitan Region. Perhaps important information could have been established in the non-licensed category. This was countered by simplifying the questions formulated for the questionnaires such that they provided an objective feedback which fitted all type of such institutions.

Data collection tools and procedures such as questionnaires, interviews and observations were limited to volunteers. In some instances, the respondents requested for more time; above a month but still would not have completed the questionnaires. This was overcome by reassuring the respondents that any data gathered was strictly to be used for academic purpose. Steady follow-up was also done to remind the respondents over the urgency of questionnaires. The participants were also given surety that the intention of the study was to add value to their area of performance. Data analysis methods which included scatter plots and correlation tables were limited to accuracy of data gathered. This was overcome by checking through questionnaires and following up on respondents in the event it prompted for a repeat of data gathering.

3.8 Ethical Considerations

Ethical consideration was done preliminarily since the problem area revolves about a sensitive subject of fraud. Fraud is a vice which probably subjected the respondents to fear of disclosing information to expose their organization. IS policy framework study was equally a sensitive area since this are formulated in parallel with sensitive processes. Therefore, consultation of the Credit Unionsô authorities was done to request for permission and respondents were required to voluntarily participate. Permission from Chief Executive Officers (CEOs) was sought before commence of study within the Credit Unions. Other senior management administrators next in position were consulted where the CEOs could not be reached. Data collected within these institutions was also treated with confidentiality.

CHAPTER FOUR: DATA ANALYSIS, PRESENTATION AND INTERPRETATION

The findings were based on 125 returned questionnaires from employees who work in Credit Union within Nairobi Metropolitan Region. 72.1% of the respondents came from Nairobi followed by Kiambu at 11.6%. Respondents from Machakos Metro region could not be reached while Kajiado had no licensed D.T SACCOs. This translated to a feedback rate of 83.7% from the respondents.

Table 4.1: Credit Unions in Nairobi Metropolitan Region.

	Metropolitan region	County	Frequency	Percent
1.	Core Nairobi	Nairobi	31	72.1
2.	Northern Metro	Kiambu	5	11.6
3.	Southern Metro	Kajiado	-	-
4.	Eastern Metro	Machakos	0	0
5.	Total		36	83.7

4.1 Demographic Information

The total number of questionnaires administered to the respondents was 140 of which 125 were returned for analysis. Background information included gender, age, education level, duration of service and department. This was for general information as tabulated in table 4.2.

Table 4.2: Background information of the respondents

			Frequency	**Percent**
Response rate	1.	Issued	140	100.0
	2.	Returned	125	89.3
	3.	Not returned	15	10.7
Gender	1.	Male	74	59.2
	2.	Female	51	40.8
Age	1.	Below 20 years	0	0.0
	2.	21-30	40	32.0
	3.	31-40	63	50.4
	4.	41-50	15	12.0
	5.	Above 50 years	7	5.6
Education level	1.	Certificate	9	7.2
	2.	Diploma	17	13.6
	3.	Undergraduate	66	52.8
	4.	Postgraduate	29	23.2
	5.	Other	4	3.2
Duration of service	1.	Less than 1 year	11	8.8
	2.	1 ï 3 years	58	46.4
	3.	4 ï 7 years	18	14.4
	4.	8 ï 11 years	8	6.4
	5.	Over 11 years	30	24
Departments	1.	Accounts & Finance	42	33.6
	2.	Administration	20	16
	3.	Audit	14	11.2
	4.	Business Management, Development & operations	6	4.8
	5.	FOSA & WSF	20	16
	6.	ICT	21	16.8
	7.	Marketing	2	1.6

Table 4.3: Levels of implementation of IS policy framework, detected and potential fraud

	Implementation_level of IS policy framework		**Detected_fraud_level**		**Potential_fraud_level**	
Level	Frequency	Percentage	Frequency	Percentage	Frequency	Percentage
10	8	6.4	8	6.4	5	4
9	12	9.6	9	7.2	9	7.2
8	27	21.6	20	16	9	7.2
7	19	15.2	17	13.6	13	10.4
6	25	20	14	11.2	16	12.8
5	24	19.2	26	20.8	27	21.6
4	4	3.2	13	10.4	14	11.2
3	3	2.4	11	8.8	20	16
2	3	2.4	4	3.2	6	4.8
1	-	0	3	2.4	6	4.8
55	125	100	125	100	125	100

Implementation Level of IS Policy Framework

Level of implementation of IS policy framework was established basing on quantifiers listed by the researcher on a table. This was scored in the questionnaire using a likert scale ranging from 1 to 10, where the highest score indicated that all the quantifiers existed.

Table 4.4: Table of implementation level of IS policy framework

Quantifier	**Level weight**	**Percentage weight**
Consistency in counseling, disciplinary action like a warning or dismissal.	1	10
Training	1	10
Alignment	1	10
Responsibilities	1	10
Revision and update	1	10
Impact; personal and organizational	1	10
Acceptance by employees	1	10
Awareness	1	10
Approval of documentation by Management	1	10
Documentation level	1	10
Total	10	100

92% of the respondents scored five and more quantifiers which is equivalent to an implementation level of 50% and more. Respondents translating to 21.6% indicated that the policy framework was implemented at a level of 80%; since they had scored eight quantifiers. Figure 2 show a chart of implementation level of IS policy.

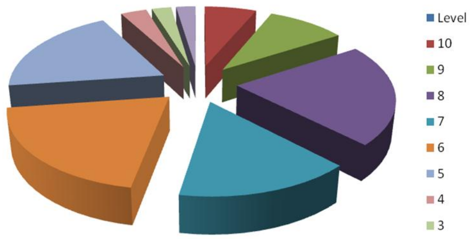

Figure 2: Implementation level of IS policy framework

Ten quantifiers were used to measure the level of fraud. A score of ten indicated that the fraud level was at 100% and the scale varied to the lowest level of a score of one indicating fraud level of 10%. Feedback from the respondents was based on this scale as shown in Table 4.5.

Table 4.5: Table of fraud level

Quantifier	**Level weight**	**Percentage weight**
Identity theft	1	10
Direct payments fraud	1	10
Lapping; payment made on one customerôs account is applied to another customerôs account where payments had previously been diverted.	1	10
Write-offs	1	10
Diversion of payments	1	10
Payroll and allowances adjustments	1	10
Fraudulent financial statements and records	1	10
Frequent changes in accounting estimates	1	10
False documentation	1	10
Exploiting Information	1	10
Total	**10**	**100**

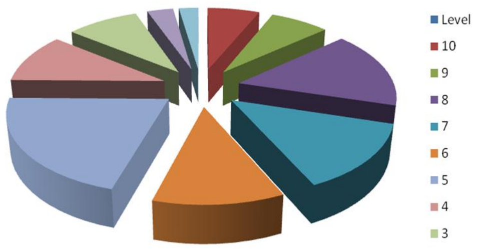

Figure 3: Detected fraud level

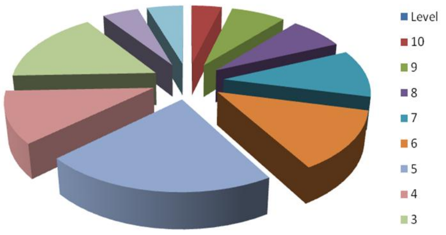

Figure 4: Potential fraud level

From figure 3 it was realized that 75.2% of the respondents scored five and more quantifiers from the ten; which indicated fraud level of 50% and more. Figure 4 displayed that the highest number of respondents translating to 22% indicated that fraud would potentially happen at a level of 50%. 21.6% also indicated that fraud would likely happen at a level of 50%. It was noted that 63% of the respondents pointed out that the fraud level was above 50%.

Further analysis of the questionnaires established findings about various perceptions of the respondents concerning the following: fraud problem, importance of IS framework, policy framework use to control fraud and fraud by employees. These were presented in tables and pie charts.

Table 4.6: Perceptions concerning fraud

	Fraud problem		Importance of IS policy Framework		Policy Framework use to control fraud		Fraud by employees	
Level	Frequency	Percentage	Frequency	Percentage	Frequency	Percentage	Frequency	Percentage
5	96	77	105	84	72	58	70	56
4	20	16	16	13	46	37	38	30
3	8	6	3	2	4	3	12	10
2	1	1	1	1	3	2	3	2
1	0	0	-	0	-	0	2	2
	125	100	125	100	125	100	125	100

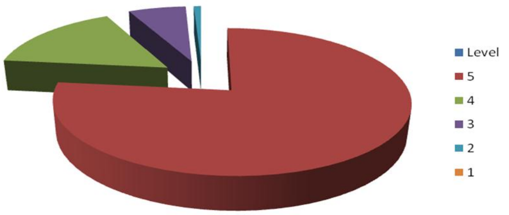

Figure 5: Fraud problem

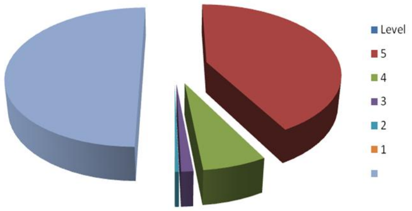

Figure 6: Importance of IS policy framework

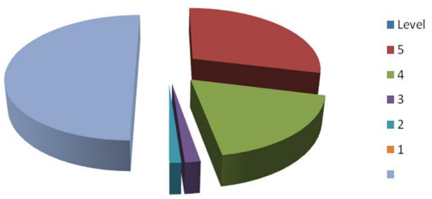

Figure 7: Policy framework use to control fraud

4.2 Data Analysis

Further analysis of the data is as shown in the scatter plot in figure 8 which indicated no correlation between Detected_fraud_level and Implementation_level of IS. Correlation analysis demonstrated from computation of Pearson Correlation and Sig. (2-tailed).

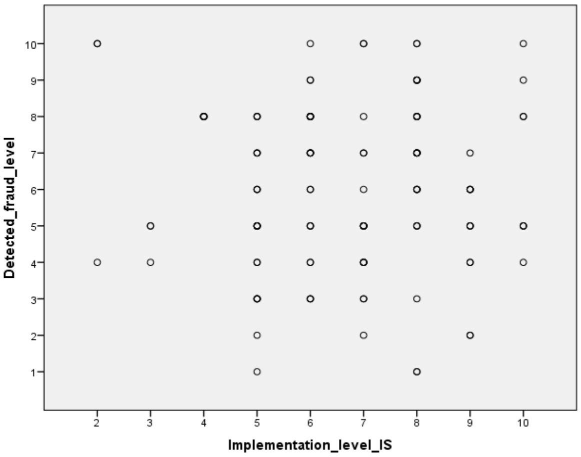

Figure 8: Scatter plot of Detected_fraud_level against Implementation_level of IS policy framework

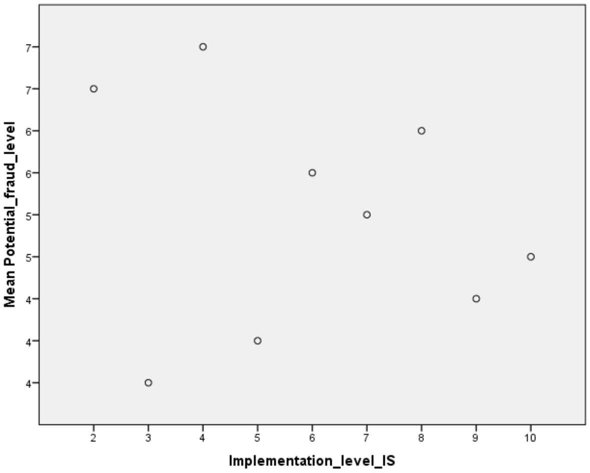

Figure 9: Scatter plot of Potential_fraud_level against Implementation_level of IS policy framework

Correlation table of three variables is represented in table 4.7.

Table 4.7: Correlation between IS policy framework, detected and potential fraud levels

Correlations

		Implementation_level_IS Policy framework	Detected_ fraud_level	Potential_ fraud_level
Implementation_level_IS Policy framework	Pearson Correlation	1	.011	-.082
	Sig. (2-tailed)		.902	.364
	N	125	125	125
Detected_fraud_level	Pearson Correlation	.011	1	.644**
	Sig. (2-tailed)	.902		.000
	N	125	125	125
Potential_fraud_level	Pearson Correlation	-.082	.644**	1
	Sig. (2-tailed)	.364	.000	
	N	125	125	125

**. Correlation is significant at the 0.01 level (2-tailed).

Table 4.7 showed how two variables namely: Implementation_level of IS and Detected_fraud_level correlated. The Pearsonôs (r) of 0.11 is closer to 0 than 1 which indicated a weak relationship. This meant that when the level of implementation of IS policy framework increased within the Credit Unions; there was no significant change in level of detected fraud. This was a likely indication that the policies were not well implemented from our respondentsô feedback since it was expected that they would control fraud levels significantly. The tailed Sig (2-Tailed) value of 0.902 also was greater than 0.05 which indicated no significant correlation between the two variables.

A negative correlation between two variables namely: Implementation_level of IS policy framework and Potential_fraud_level could also be established. This was from the Pearsonôs (r) value of -0.82 which signified a negative correlation. It implied that an increase in the level of implementation of policies reduced the level of fraud expected to occur in the near future. The tailed Sig (2-Tailed) value of 0.364 was greater than 0.05 which implied a negative correlation between the two variables.

The data analysis methods were justified since the nature of relationship between the level of implementation of IS policy framework with the level of fraud were key elements. The outcome indicated that higher implementation level of IS policy framework would result to reduction of the potential fraud levels. The results also indicated that the implementation level of IS policy framework had a weak correlation with the level of fraud. This necessitated the need to apply a different way of implement IS policy framework which can be done by applying the Zachmanôs framework.

4.3 Hypothesis Testing

The hypothesis stated that, ñImplementation level of IS policy framework has no significant influence on reduction of potential fraud levels in Credit Unionsò. This was a null hypothesis H0: which was equivalent to saying coefficient; r = 0. From the correlation between Implementation_level of IS and the Potential_fraud it was noted that the Pearsonôs value (r) -0.082 was a negative value. This was equivalent to saying coefficient; r Í 0. Basing on this findings an alternative hypothesis; H1: Implementation level of IS policy framework has significant influence on reduction of potential fraud levels in Credit Unions was justified (equivalent to saying coefficient; r Í 0).

4.4 Comparison of Results with Literature Reviewed

63.2% of the respondents indicated that enough effort had not been done to reduce fraud in the Credit Unions. 97.6% of agreed that an IS Policy framework resultant from this study could be tried in their organizations. It was also realized that 100.0% of the institutions had in place both an IS and policies. All the institutions covered had experienced fraud cases with a likelihood of future reoccurrence even though policies were in place. This demonstrated that more should be done to control fraud through formulation of the right IS Policy framework which this research sought to address.

4.5 Implication of Results

It was observed from the results that low level of implementation of policies resulted to high fraud rate and higher chances of future occurrence of fraud as tested by the hypothesis. The enforcement level of the policies was also directly proportional to the impact level. This indicated that the policies were structured in a way which necessitated application of the Zachmanȋs framework to aid in the implementation. The level of fraud which had occurred was proportional to the level of fraud yet to occur in later days. This prediction implicated that controls could be implemented to manage potential fraud incidences. IS policy framework if well implemented was meant to supplement guidance on access. Policies ensured existence of enforcements on accounts during login such as restricted login by time of day, day of week, or location. Access control policies like the identity based policies, also were both role and attribute based and would secure an IS as documented in the United States National Institute of Standards and Technology (2012). Zachmanȋs framework as used in this study would provide such guidance.

4.6 Testing of the Zachman Framework

The framework was tested and two phases used to test standards were applied which included: verification and validation basing on Witherell, Rachuri, Narayanan & Lee (2013). Verification testing sought to justify if the intentions of the framework met all the areas addressed by an IS policy. It was realized that from the point of intersections of the 6x6 matrix represented an enterprise as a whole. All the functions and departments of the Credit Union were represented in this making it practical to use. Validation testing pointed out how the policies developed in the Credit Unions could be structured and made operational within the matrix intersections which made it possible to deploy the framework.

Scope and consistency testing also indicated that the goals of the framework were aligned to the expectation of any organization. There was conformance to other standards to fulfill strategic corporate goals of the organizations. Consistency was seen while tracing the logical and physical models in each column correctly which lead to the contextual and conceptual bases in the top rows of the framework. The two dimensions offered by the Zachman framework allowed analysis of various aspects of the standard and correspondence was noted between the standardȋs high-level goals and its logical, physical, and detailed models. Conformity assessment was in addition done and the results were analyzed from the interview feedback from the respondents. This was achieved from first party assessment or self-certification which was performed and the respondents were allowed to give their opinions.

4.7 Contribution of Results

The results validated that the problem area still requires attention. Basing on the analysis of the feedback from all the respondents, it was noted averagely that the implementation level of IS policy framework stood at 67%. This indicated that fraud which had already occurred and the potential fraud were at levels of 60% and 52% respectively. A total of 54.4% of the respondents gave suggestions on how application of IS policy framework would be implemented to control fraud which was important to be used in application of the Zachmanôs framework. It was noted that 100% of the respondents indicated their organizations had documented policies but on the contrary fraud levels were noted to be prevalent.

CHAPTER FIVE: CONCLUSIONS AND RECOMMENDATIONS

5.1 Achievements

The four objectives as stated were met from the research outcomes as follows:

1. *To establish the level of implementation of IS policy framework by the Credit Unions.*

   Feedback received pointed out that IS policy framework existed in all the Credit Unions. 92% of the respondents indicated that the level of implementation of IS policy framework was at 50% and more while 8% scored the level at less than 50%. All the licensed Credit Unions covered had the IS policy framework in place. However, it was realized that the level of implementation of these policies was inadequate such that the desired impact was not fully met.

2. *To determine the extent of fraud occurrence on IS within the Credit Unions.*

   All employees interviewed within the Credit Unions admitted that fraud was prevalent. 100% of the respondents confirmed that fraud occurred. It was also noted that some employees were engaged in fraudulent activities within these institutions.

3. *To determine the potential fraud level exposure to the IS within the Credit Unions.*

   An indication from the results showed high possibility of occurrence of fraud in the near future assuming the current status was maintained within the Credit Unions. 63% of the respondents indicated that fraud would happen at a level above 50%. These findings confirmed the third objective.

4. *To identify and apply a framework for implementation of IS policy for the Credit Unions.*

   This objective was achieved by selecting the Zachman framework to aid in the implementation of IS policies. This was achieved through deploying a 6x6 matrix as an implementation framework in which all the existing policies would be incorporated.

5.2 Limitations

Limitations faced revolved about the objectives which seemed to be a sensitive area of study. The respondents felt insecure to providing information about fraud. It was not also possible to tell if those contacted were fraudulent thus restrain some information. It was only through the permission of CEOs or the top Management who could give a go ahead for gathering any information within the Credit Unions. However, this was tackled by re-assuring the participants that any information gathered would exclusively be used for academic purpose. Transmittal letters also were done to initiate further deliberation.

5.3 Conclusion

This study resulted to use of the Zachmanȏs framework to implement IS policies. This was achieved by implementing the policies in-line with the 36 matrix elements as indicated in appendix iv. It was realized that all the IS policies from Credit Unions could be against the abstraction columns and the rows. The elements addressed various issues within the organizations which interacted with IS. This study contributed value to various stakeholders. To the Industry, it stood to benefit since there was clarity between the policy developers and those who were in charge of monitoring and implementation. Zachmanȏs framework displayed a function matrix about people who were important to the business and defined their roles in relation to the policies. There was a guideline to enhance proper documentation of policies and a follow-up on their implementation. The stakeholders were therefore incorporated to aid in the implementation of policies making it possible to realize the desired impacts. The issue of fraud against the IS could therefore be controlled which was a threat leading to lose of value within the organizations. Fraud control was also valuable to the Revenue collectors and the Society. Primary data acquired from the respondents displayed the actual situation as it occurred at their institutions for analysis. This contributes academically and can be used as secondary data by other researchers who may wish to build on this study. The use of the elements of the Zachmanȏs framework also contributes academically for development various areas of study.

5.4 Recommendations

Presence of IS policies as studied was not sufficient to control fraud in organizations. It is only when a suitable framework is used to implement the policies that the desired impact can be felt. It is recommended that developed policies in IT and other departments within organizations could be implemented using the choice framework as displayed in this research. The framework is not only limited to IS policies in Credit Unions but can also be used at a broader perspective in various organizations.

REFERENCES

1. Askarov, A. & Chong, S. (2012). Learning is Change in Knowledge: Knowledge-based Security for Dynamic Policies. *Proceedings of the 25th IEEE Computer Security Foundations Symposium (CSF).* June 2012. p. 308ï 322.
2. Brooks, P., (2012). Metrics for Service Management: *Designing for ITIL*. Van Haren: Zalbommel.
3. Cameron, B. H., & McMillan, E. (2013) Analyzing the Current Trends in Enterprise Architecture Frameworks. *Journal of Enterprise Architecture*. February. [Online]. Available from: http://ea.ist. psu.edu/documents/journal_feb2013_cameron_2.pdf. [Accessed: 27th November 2014].
4. Kenya Economic Report. (2013). Kenya Institute for Public Policy Research and Analysis, (KIPPRA). *Creating an Enabling Environment for Stimulating Investment for Competitive and Sustainable Counties.*
5. ISO. (2013). International Standard (ISO/IEC27002). *Information technology - Security techniques - Code of practice for information security controls.* Switzerland.
6. Lin, C., Song, F. M. & Sun, Z. (2011). *The Financial Implications of Corporate Fraud.* [Online] Available from:http://www.fin.ntu.edu.tw/~conference/conference 2012/ proceedings /files/A193_Financial%20implications%20of%20fraud_Nov_01.pdf. [Accessed: 27th November 2014].
7. Morgan, J. P. (2013). Association for Financial Professionals. *2013 AFP Payments Fraud and Control Survey Report of Survey Results*   [Online]. Available from: http://www.larutech.com /jan2014/2013_AFP_Payments_Fraud_Survey.pdf . [Accessed: 27th November 2014].
8. Morgan, J. P. (2014). Association for Financial Professionals.   2014 AFP Payments Fraud and Control *Survey Report of Survey results.* [Online]. Available from:https://www.jpmorgan.com/cm/BlobServer/2014_AFP_Payments_Fraud_Survey.pdf?blobkey=id&blobwhere=1320639355606&blobheader=application/pdf&blobheadername1=CacheControl&blobheadervalue1=private&blobcol=urldata&blobtable=Mungo Blobs. [Accessed: 27th November 2014].
9. Munkner, H-H. (2013). Worldwide regulation of co-operative societies ï an Overview. *European Research Institute on Cooperative and Social Enterprises Working Paper.* [Online] 53 (3). p 13. Available from:http://euricse.eu/sites/euricse.eu/files/db_uploads/ documents/1371044429_n2351.pdf [Accessed: 27th November 2014].

10. Polikandrioti, M., Goudevenos, I., Michalis, L., Nikolaou, V., Dilanas, C., Olympios, C., Votteas, V., Elisaf, M., (2011). Validation and reliability analysis of the questionnaire ñNeeds of hospitalized patients with coronary artery diseaseò. *Health Science Journal.* [Online] 5 (2). p. 137ï 148. Available from:http://hypatia.teiath.gr/xmlui/bitstream/handle/11400/1287/527.pdf?sequence=1 [Accessed: 27th November 2014].
11. Radwan, A. & Aarabi, M. (2011). Study of Implementing Zachman Framework for Modeling Information Systems for Manufacturing Enterprises Aggregate Planning. *Proceedings of the 2011 International Conference on Industrial Engineering and Operations.* Kuala Lumpur, Malaysia. January 22 ï 24, 2011. [Online]. Available from: http://www.academia.edu/990285/Study_of_ Implementing_Zachman_Framework_for_Modeling_Information_Systems_for_Manufacturing_Enterprises_Aggregate_Planning [Accessed: 27th November 2014].
12. SASRA. (2011). *SACCO Supervision Annual Report 2011, (Deposit Taking SACCOs), SACCO Societies Regulatory Authority (SASRA).*
13. SASRA. (2012). *SACCO Supervision Annual Report 2012, (Deposit Taking SACCOs), SACCO Societies Regulatory Authority (SASRA).*
14. SASRA. (2013). *SACCO Supervision Annual Report 2013, (Deposit Taking SACCOs), SACCO Societies Regulatory Authority (SASRA).*
15. The open group. (2014). [Online]. Available from: http://pubs.opengroup.org/architecture/ togaf8-doc/arch/ [Accessed: 27th November 2014].
16. United States. National Institute of Standards and Technology. (2012). *Trend Micro Products (Deep Security and Secure Cloud).* [Online] Available from: http://www.trendmicro.com/cloud-content/us/pdfs/business/oth_fisma-nist-solution-profile.pdf. [Accessed: 27th November 2014].
17. Waema T, M. & Ndungôu N, M. (2012) Evidence for ICT Policy Action Policy. *Understanding what is happening in ICT in Kenya.* Policy Paper 9, 2012. [Online]. Available from:http://www.researchictafrica.net/publications/Evidence_for_ICT_Policy_Action/Policy_Paper_9_-_Understanding_what_is_happening_in_ICT_in_Kenya.pdf [Accessed: 27th November 2014].
18. Wanyama F.O. (2009). *Surviving Liberalization: The Co-operative Movement in Kenya*, International Labour Organization. Coop Africa Working Paper No.10. [Online] Available from:http://ilo.org/public/english/employment/ent/coop/africa/download/wp10_survivingliberazation.pdf [Accessed: 27th November 2014].

19. Warfield, B. (2013). *Employee Fraud in Australian Credit Unions.* [Online] Available from: http://www.warfield.com.au/Warfield_Employee_Fraud_in_Australian_Financial_Institutions.pdf [Accessed: 27th November 2014].
20. Witherell, P., Rachuri, S., Narayanan, A., Lee, J.H., (2013). *FACTS: A Framework for Analysis, Comparison, and Testing of Standards.* U.S. Department of Commerce: National Institute of Standards and Technology. [Online] Availablefrom:http:// nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7935.pdf [Accessed: 27th November 2014].
21. World Council of Credit Unions. (2014). *What is a Credit Union?* [Online] Available from: http://www.woccu.org/about/creditunion. [Accessed: 27th November 2014].
22. Zhang, S., & Le, F. H. (2013). An Examination of the Practicability of COBIT Framework and the Proposal of a COBIT-BSC Model. *Journal of Economics.* [Online] 1 (4). Available from: https://openaccess.leidenuniv.nl/bitstream/handle/1887/24618/84-021.pdf?sequence=1. [Accessed: 27th November 2014].

APPENDICES

Appendix I: Structured Questionnaire

My name is Samuel O. Lubanga, Reg. No. P54/65722/2013. I am undertaking a MSc.

Course in IT Management of the University of Nairobi. This study is a project entitled

Sample Framework of Information Systems Policy for fraud control in Credit Unions.

Instructions: Please answer the following questions in section **A, B and C** by marking the relevant box with a tick (ã) or writing down your answer in the space provided where applicable.

Confidentiality: The responses you provide will be strictly confidential. No reference will be made to any individual(s) in the report of the study.

Section A: Background information

This section of the questionnaire refers to background information. Although we are aware of the sensitivity of the questions in this section, the information will allow us to compare groups of respondents.

1. What is your gender? [ ] Male [ ] Female
2. In which of the following age brackets do you belong?

   [ ] Below 20 years [ ] 21- 30 years [ ] 31- 40 years [ ] 41-50 years [ ] Above 50 years
3. What is your education level (state the highest level?)

   [ ] Certificate [ ] Diploma [ ] Undergraduate [ ] Post Graduate [ ]Other ____________
4. How many years have you worked with the company?

   [ ] Less than 1 year [ ] 1-3 years [ ] 4-7 years [ ] 8-11 years [ ] Over 11 years
5. What is your career orientation?

   [ ] Accounts [ ] Marketing [ ] Business Management [ ] IT Professional [ ] Technical

   [ ] Other ______________
6. Kindly indicate your department ________________________________

Section B: IS

This section of the questionnaire explores application of IS policy framework in your organization.

7. Does your organization have an IS (this could refer to the information and communication technology (ICT) that an organization uses in support of business processes such as ERPs and MIS)? Yes[ ] No[ ]
8. Are there policies in place governing the use of the IS? Yes [ ] No [ ]

   If yes, in a scale of 1 to 10; where 10 is the highest score, complete the grid by a tick (ã) as appropriate on your perception about the policies.

		1	2	3	4	5	6	7	8	9	10
1.	Documentation level										
2.	Level of awareness										
3.	Enforcement level										
4.	Impact level										

9. Please indicate your level of agreement of the importance of an IS Policy frame work from a scale of one to five, where; 5 = strongly agree, 4 = agree, 3 = neutral, 2 = disagree and 1 = strongly disagree, please indicate your level of agreement by a tick (ã).

		1	2	3	4	5
1.	IS policy frame work is important					

Section C: Fraud Concerns

10. The following are perceived indicators of fraud in Credit Unions. Please indicate your level of agreement. On a scale of one to five, where; 5 = strongly agree, 4 = agree, 3 = neutral, 2 = disagree and 1 = strongly disagree, please indicate your level of agreement to the challenges below;

		1	2	3	4	5
1.	Fraud is a problem which needs to be dealt with					
2.	A policy framework can be used to control fraud					
3.	Fraud is likely to be committed by employees within the organization					

11. In a scale of 1 to 10; where 10 is the highest score, complete the grid by a tick (ã) as appropriate on your perception about fraud level in Credit Unions.

		1	2	3	4	5	6	7	8	9	10
1.	Fraud level										

12. In a scale of 1 to 10; the least to highest score respectively, complete the grid by a tick (ã) as appropriate on your opinion on the likelihood of fraud to occur in your organization.

		1	2	3	4	5	6	7	8	9	10
1.	Likelihood of fraud										

13. Do you think that enough has been done to contain fraud in Credit Unions? Yes[ ]No [ ]
14. Given a suggested IS policy framework from this study, would you wish it tried out in your organization? Yes [ ] No [ ]
15. Please give any suggestions or recommendations on how application of IS policy framework can be implemented to control fraud.______________________________

____

Cell phone: 0723 848 045, email samlubanga@gmail.com

Thank you for your co-operation in completing this questionnaire.

Appendix II: DT Credit Unions Within Nairobi Metropolitan Region

	Category	Place	Name	Address	Contact person (CEO/Representative)
1	Large	Nairobi	Mwalimu National Sacco Society Ltd	62641-00200 Nairobi Mwalimu Co-op House, Tom Mboya Strt	Mr. Robert Shibutse
2	Large	Nairobi	Harambee Sacco Society Ltd	47815-00100 Nairobi Co-operative Plaza, Haile Selassie Avenue/Uhuru Highway, Round-about	Mrs Gladys Gichohi/ Pamela
3	Large	Nairobi	Afya Sacco Society Ltd	11607 - 00400, Nairobi. Afya centre, Tom Mboya street	Deputy CEO Felix
4	Large	Nairobi	Stima Sacco Society Ltd	75629-00100 Nairobi Stima Sacco Plaza, Mushembi Road	Mr. Paul Wambua/ Alice
5	Large	Nairobi	Kenya Police Sacco Society Ltd	51042-00200 Nairobi	Simon K. Tanui: Gen Man
6	Large	Nairobi	UN Sacco Society Ltd	30552-00100 Nairobi U.n Sacco Building, Un Avenue, Off Limuru rd	Clement Tongi/ Evelyne
7	Large	Nairobi	Ukulima Sacco Society Ltd	44071-00100 Nairobi Ukulima House, Haile Selassie Road	Mr. Henry E. Nakaya
8	Large	Nairobi	Kenya Bankers Sacco Society Ltd	73236-00200 Nairobi Kenya Bankers Sacco Center, 3rd Ngong Avenue	Elijah Dede
9	Medium	Kiambu	Metropolitan Sacco Society Ltd	871-00900 Kiambu Community Centre, Biashara Street	Francis Kamau Nganga
10	Medium	Nairobi	Magereza Sacco Society Ltd	53131-00100 Nairobi Mageso Chambers, Moi Avenue	Augustine Mutisya; DCEO
11	Medium	Nairobi	Hazina Sacco Society Ltd	59877-00100 Nairobi Kibera Road Off Ngong Road Behind Kobil Petrol	Daniel C. Kimwama
12	Medium	Nairobi	Nacico Sacco Society Ltd	34525-00100 Nairobi NACICO Plaza, Landhis Road	Timothy B. Vikiru, Finance Manager
13	Medium	Nairobi	Sheria Sacco Society Ltd	34390-00100 Nairobi Sheria Sacco House, Off Matumbato Street	Kenneth Ondiala
14	Medium	Machakos	Masaku Teachers	Masaku Teachers Sacco Ltd, Machakos P.O Box 818 Machakos	
15	Medium	Kiambu	Kiambu Unity Finace Co-Op Union	P.O.Box 268-00900, Kiambu Mapa Hse, 8th Flr Biashara St, Karuri, Kiambu	
16	Medium	Nairobi	Waumini Sacco Society Ltd	66121-00800, Waumini House, Westlands	Christine Owande
17	Medium	Nairobi	Chuna Sacco Society Ltd	30197-00100 NAIROBI Old Boiler House, Harry Thuku Road	Edward Tale Nabangi
18	Medium	Nairobi	Jamii Sacco Society Ltd	57929-00200 Nairobi Jamii Sacco Court, Mukenia Road Physical Location Jamii Sacco Court Mukenia Road, South ớBô Next to Mater Hospital	Mr Eliud Chepkwony
19	Medium	Nairobi	Chai Sacco Society Ltd	278-00200 Nairobi KTDA Plaza, Junction Of Moi Avenue/Ronald Ngala	Purity Mungure Maina
20	Medium	Nairobi	Maisha Bora Sacco Society Ltd	30062-00100 Nairobi Unilever Kenya Ltd Office, Commercial Street	Samuel Ngure
21	Medium	Nairobi	Kenpipe Sacco Society Ltd	314-00507 Nairobi.	Mwasambu Mbago
22	Medium	Nairobi	Naku Sacco Society Ltd	78355-00507, Nairobi Liberty Plaza, Mombasa Road 66827-00800 Nairobi	Edwin Kinyua
23	Medium	Nairobi	Safaricom Sacco Society Ltd	Safaricom House, Waiyaki Way	George Ochiri Onyango/ Nicholas ITM
24	Medium	Nairobi	Nassefu Sacco Society Ltd	43338-00100 Nairobi Nssf Building (Block C), Bishop Road	Malingi Dzombo
25	Small	Nairobi	Wanaanga Sacco Society Ltd	34680-00100 Nairobi Meteorological Hq, Ngong Road	Mr. Vincent Rota denis
26	Small	Nairobi	Nation Sacco Society Ltd	P.O. Box 22022-00400 Nairobi Cambrian, Moi Avenue	Jacob Kimathi/ Moses
27	Small	Nairobi	Mwito Sacco Society Ltd	56763-00200 Nairobi Mwito House, Desai	Mr. George M.

				Road	Mugambi
28	Small	Kiambu	Kenya Canners Sacco Society Ltd	P.O.BOX 1124-01000 Thika Kenya Canners Sacco Building, Wabera street	Chairman: DM Kioi
29	Small	Nairobi	Tembo Sacco Society Ltd	91-00618 Ruaraka Tembo Complex, Mukima Drive	Ms. Lydia Mungai
30	Small	Nairobi	Comoco Sacco Society Ltd	3015-00100 Nairobi Cmc Building, Lusaka Road	Mr Richard Ombai
31	Small	Kiambu	Githunguri Dairy Sacco Society Ltd	896-00216 Githunguri Dairy Farmers Co-op Society Building, Market Street	Kioko
32	Small	Machakos	Universal Traders Sacco Society Ltd	2119-90100 Machakos Traders House, Syokimau House	Kisili Stephen Kioko
33	Small	Nairobi	Airports Sacco Society Ltd	19001-00501 KAA Complex, J.K.I.A.	Cheruiyot Kipsol
34	Small	Nairobi	Kingdom Sacco Society Ltd	8017- 00300, Nairobi	Dalmas .J. Menya
35	Small	Kiambu	Nrs Sacco Society Ltd	575-0092 Kikuyu	Joan Mbesya
36	Small	Nairobi	Nafaka Sacco Society Ltd	30586-00100 Nairobi Nyumba Ya Nafaka, Enterprise Road	Nyaga Moses Njiru/ Rose
37	Small	Kiambu	Dimkes Sacco Society Ltd	886-00900 Kiambu Bishop Maua House, Kiambu/Ndumberi Road Bishop Magua House Second Floor	Mbogo Samuel Ndichu/ Rita
38	Small	Kiambu	Jijenge Sacco Society Ltd	6222-00100 Thika Wangu House, Uhuru Street,Thika	Dishon Kairu, Statutory Manager
39	Small	Kiambu	Fariji Sacco Society Ltd	589-00216 Githuguri Diplomat House	Josphine Thiongo
40	Small	Kiambu	Kiambaa Dairy Rural Sacco Society Ltd	669-00219 KARURI Kiambaa Dairy Farmers Bld, Karuri	Monica W. Muiruri
41	Small	Nairobi	Orthodox Sacco Society Ltd	43582-00100 Nairobi Odesa Sacco Building, Kawangware Road	David Osotsi
42	Small	Nairobi	Wanandege Sacco Society Ltd	19074-00501 Nairobi Wanandege Plaza, Embakasi Road	James Murithi/ Susa
43	Small	Nairobi	Kenversity Sacco Society Ltd	10263-00100 Nairobi Mizpah House, Kahawa Sukari Strt	Alfred Korir/ Kirui

Appendix III: Summary of Data Collected

Respondent number	Have IS	Policy documentation level	Policy awareness level	Policy enforcement level (Implementation_level 0f IS policy framework)	Policy impact level	Importance of IS policy framework	Fraud problem	Policy framework use to control fraud	Fraud by employees	Detected_fraud_level (incidences of fraud already occurred)	Potential_ fraud_level (anticipated fraud incidents likely to occur)	Enough effort have been done to control fraud	Choice to implement an IS policy framework	Suggestions to implement IS policy frameworks in organizations.
1	Y	8	4	5	5	5	5	4	5	3	4	N	Y	Awareness
2	Y	7	8	8	8	5	4	2	5	6	6	y	y	
3	Y	7	6	8	8	5	5	5	5	8	8	y	y	
4	Y	7	9	7	9	5	5	5	5	10	5	N	Y	
5	Y	7	7	7	7	5	5	5	5	4	4	N	Y	
6	Y	7	8	5	5	5	4	4	5	4	5	N	Y	
7	y	8	6	5	7	5	5	5	3	5	5	y	y	
8	y	8	5	5	5	5	5	4	4	7	5	N	Y	
9	Y	9	6	6	7	5	5	4	4	6	3	N	Y	Strict user policy on security and system use
10	Y	9	7	6	6	5	5	4	4	5	6	N	Y	
11	Y	10	8	5	5	5	3	4	5	1	1	N	Y	Some IS can be used to seal loopholes which may aid fraud.
12	Y	8	7	7	9	5	5	3	4	5	5	N	Y	Audit trail, access controls, automation of processes
13	Y	10	9	9	9	5	5	4	4	6	4	N	N	Putting system controls in place, audit trails, setting a role centre for assigning roles in the system to control the users.
14	Y	7	5	5	6	5	5	5	5	2	1	Y	Y	
15	Y	5	4	5	6	5	5	4	5	8	7	N	Y	The policy gives a guideline, stringent control and frequent monitoring of loopholes and gaps in what can reduce their likelihood of fraud
16	Y	6	4	4	5	5	5	5	5	8	5	N	Y	
17	Y	10	9	8	10	5	5	5	2	1	1	Y	Y	
18	Y	9	8	8	9	5	5	5	5	5	5	N	Y	
19	Y	8	9	9	9	5	5	5	5	6	7	Y	Y	
20	Y	6	7	7	7	4	4	4	5	3	5	N	Y	
21	Y	10	7	8	8	5	3	5	4	3	2	Y	Y	The policy framework should define guidelines that facilitate implementing controls at various levels to ensure no individuals or group of individuals can collude at ease to commit fraud.
22	Y	8	8	5	5	5	5	5	5	8	3	N	Y	By training and creating awareness

23	Y	8	7	8	8	5	4	4	5	6	6	N	Y	Formulating policies that avoid fraud, eliminating collision in an organization.
24	Y	8	7	8	7	5	4	5	4	7	6	Y	Y	Exceptional reports, which give critical analysis of important events in the IS process
25	Y	8	6	6	7	4	5	4	4	6	6	Y	Y	Continuous evaluation & improving of control systems
26	Y	8	7	6	7	5	4	5	4	8	6	Y	Y	Control of user rights & access to information
27	Y	8	7	7	8	5	4	4	5	7	6	Y	Y	Internal control systems
28	Y	7	7	7	8	5	5	4	4	5	6	Y	Y	Instituting interior strong control systems
29	Y	7	6	7	7	5	5	4	4	7	6	Y	Y	Control systems
30	Y	10	9	9	9	5	5	4	4	7	7	N	Y	Proper documentation of incidences & policies, follow-up reports to be generated periodically.
31	Y	10	10	10	10	5	5	5	5	5	3	N	Y	Involve all stakeholder/ user at every step of formation and implementation.
32	Y	9	10	10	8	5	5	5	4	5	4	N	Y	Employer should engage professionals.
33	Y	10	10	10	10	5	5	5	4	4	1	N	Y	Frequent Systems audits
34	Y	9	7	8	9	5	5	4	4	7	3	N	Y	
35	Y	7	6	6	7	5	5	5	5	9	7	Y	Y	By putting more controls in IT sections related cases
36	Y	8	6	6	8	5	3	4	5	3	4	Y	Y	
37	Y	10	10	10	10	5	5	5	1	8	1	Y	Y	Fraud and control plan should be put in place to assess the possible loopholes that can lead to fraud.
38	Y	5	5	3	3	5	5	5	5	5	5	N	Y	Use of frequent audit reports on the application the organization is using.
39	Y	8	8	9	9	5	5	5	5	5	2	N	Y	Frequent audit
40	Y	9	9	7	8	5	5	5	5	4	5	N	Y	By use of up-to-date audit systems that can detect fraud.
41	Y	8	9	10	10	5	5	5	5	10	5	N	Y	
42	Y	8	9	9	8	5	4	4	4	6	5	Y	Y	Use of passwords and authority and center checking work done by one person by another
43	Y	7	8	6	5	3	3	2	1	8	6	Y	Y	Can be implemented by incorporating certified system analyst.
44	Y	7	5	5	5	5	5	5	5	7	4	N	Y	By adhering to the procedures in the policy
45	Y	8	8	7	6	4	3	3	5	5	8	N	Y	By use of software application MIS applications.
46	Y	10	8	8	8	5	5	5	5	5	3	Y	Y	With adequate internal control then I.S can be effective to control fraud.
47	Y	9	7	7	7	5	5	5	5	5	3	Y	Y	Allocation of necessary System rights only to respective personnel
48	Y	8	4	5	6	5	4	4	4	3	3	Y	Y	By regular check or sport audit

49	Y	8	4	5	6	5	4	4	4	3	3	Y	Y	User authentication and other security policies would be expressed as per the IS policy hence deterring chances of fraud.
50	Y	8	7	8	8	5	5	4	4	8	2	Y	Y	Educate staff and make them aware of the benefits of IS policy framework and also making controls within the system.
51	Y	9	9	9	9	5	5	5	5	2	2	Y	Y	Set standards and controls within the operating systems in the organization. Educate staff on the benefits of the same.
52	Y	8	9	8	9	4	5	5	5	9	5	N	Y	Enhanced independent vetting (extended) on regular basis i.e. quarterly each year.
53	Y	6	4	5	5	5	5	5	4	4	5	N	Y	
54	Y	9	6	9	8	5	5	4	4	4	4	Y	N	
55	Y	6	4	5	5	5	5	5	3	3	4	N	Y	An important organization should be set up to manage standards and applicability of IS
56	Y	9	8	9	9	5	5	4	4	4	2	Y	Y	
57	Y	8	6	7	5	4	4	4	3	4	3	Y	Y	
58	Y	9	4	3	5	4	4	4	4	5	3	Y	Y	
59	Y	5	6	6	6	5	4	4	4	3	2	Y	Y	
60	Y	5	5	5	5	5	4	4	4	6	5	N	Y	Upon interpretation of the framework ensure it is in use and being followed.
61	Y	9	7	7	6	5	5	5	3	2	1	N	Y	Adherence to strict internal controls on all processes within the organization.
62	Y	6	6	6	6	5	5	5	5	5	6	N	Y	
63	Y	7	7	6	5	5	5	4	3	4	3	Y	Y	Frequent monitoring and assessment of process involved.
64	Y	8	6	6	7	5	5	5	5	7	8	N	Y	
65	Y	6	10	7	10	5	5	5	5	5	5	N	Y	
66	Y	10	10	9	10	5	5	5	5	2	5	N	Y	
67	Y	9	8	8	8	5	5	4	5	6	4	N	Y	
68	Y	8	8	6	5	5	5	5	5	7	7	N	Y	
69	Y	8	8	9	8	5	5	4	3	5	5	Y	Y	
70	Y	8	3	6	8	5	5	5	5	5	6	N	Y	Reviewing the current process and ICT structure, consultation with stake holders, design and implementation of the framework and awareness of the framework.
71	Y	9	8	9	9	4	5	4	5	6	7	N	Y	
72	Y	7	9	6	9	5	5	5	5	8	4	N	Y	Ensuring that the systems are secured by disabling unauthorized personnel to access the system
73	Y	7	6	5	5	5	4	5	5	6	7	N	Y	A policy can be used to enforce system awareness and enforcement of security policies in place
74	Y	6	6	7	8	4	5	5	5	6	3	Y	Y	Should have efficient audit trail

75	Y	5	6	7	7	4	5	4	4	4	3	Y	Y	By establishing appropriate information security within the staff members. Implementing security measures that match information's value, classification and sensitivity. Adhering to all laid down regulatory requirements.
76	Y	8	2	2	7	5	5	5	4	10	8	N	Y	
77	Y	8	8	9	8	4	5	5	5	5	3	N	Y	Educating the users areas of possible risk, continuous training on fraud and risk areas in IS to u
78	Y	4	6	5	5	5	5	5	3	5	5	N	Y	Installation of modern ISP framework
79	Y	6	8	5	4	5	5	5	5	7	4	N	Y	By use of biometrics and key logs to protect vulnerable areas in the organization e.g. server rooms.
80	Y	6	8	8	8	5	4	4	4	6	5	N	Y	By restricting access to only the qualified or relevant users. By breaking down process or integrating approval codes to process. This must be approved by a manager.
81	Y	9	6	6	8	5	5	4	4	7	7	N	Y	By classification of information and limiting access to some. Identifying risk level areas, then define access to the various users
82	Y	6	7	5	8	2	2	4	2	8	9	Y	Y	Policy should have strict set of rules on management
83	Y	6	5	6	4	5	5	4	4	8	5	N	Y	
84	Y	9	9	10	9	5	5	5	4	8	8	N	Y	
85	Y	6	8	7	8	5	3	5	5	5	8	Y	N	
86	Y	3	6	6	6	5	5	5	5	4	3	N	Y	
87	Y	6	6	6	6	5	5	5	5	9	9	Y	Y	By putting in place incident management procedures and mechanism to review violations and to ensure appropriate responses in the event of security incidents breaches a failure.
88	Y	6	7	8	5	4	4	4	3	5	5	Y	Y	
89	Y	7	7	8	8	5	5	5	5	10	5	N	Y	
90	Y	8	7	6	7	5	5	5	5	7	6	N	Y	
91	Y	9	9	10	10	5	5	5	4	9	8	N	Y	
92	Y	8	10	8	8	5	4	3	3	8	3	Y	Y	Policy should have strict set rules on management with designated administrative stipulated.
93	Y	5	5	5	5	5	4	4	4	5	4	N	Y	

94	Y	8	9	10	8	5	5	5	5	5	6	Y	Y	The use of passwords is the best method to deal with the issue
95	Y	8	7	8	9	5	4	4	5	7	7	Y	Y	Offering training
96	Y	8	7	8	8	4	5	5	5	9	10	N	Y	
97	Y	6	6	4	6	5	5	5	5	8	7	Y	Y	
98	Y	8	5	5	5	5	5	5	5	5	6	N	Y	The system in place should have a reliable audit & trail & should minimize data loss
99	Y	7	8	8	8	5	5	5	5	10	7	N	Y	
100	Y	6	5	5	5	4	5	4	4	3	3	N	Y	
101	Y	4	5	2	6	5	5	5	5	10	10	Y	Y	
102	Y	6	5	7	6	4	5	4	4	3	3	N	Y	
103	Y	8	4	6	8	5	5	5	5	10	10	N	Y	
104	Y	8	6	6	7	5	5	5	5	8	8	Y	Y	
105	Y	8	5	4	5	4	5	4	2	8	9	N	Y	Access supervision for IS. Embedded system to trail suspicious or out of ordinary transactions. Reduce number of people interacting within with the system.
106	Y	5	6	5	5	5	3	3	3	5	3	N	Y	
107	Y	3	3	3	3	5	5	4	5	4	5	N	Y	
108	Y	7	6	7	6	5	5	5	5	10	9	N	Y	A well defined policy of regular system audit by qualified systems auditor for these friends to be detected in time and rectified.
109	Y	8	9	6	8	5	5	5	5	7	6	Y	Y	This can be implemented through giving right to each person and changing them over times also be imposed.
110	Y	8	8	8	8	5	5	5	5	9	9	N	Y	Having clarity between the policy developers and those who are in charge to monitor and implement.
111	Y	8	7	6	6	4	5	4	4	8	5	N	Y	Check and measure where employers contact with cash and checks is limited.
112	Y	9	6	6	6	5	5	5	5	9	9	N	Y	
113	Y	6	7	6	5	5	5	5	5	3	4	N	Y	Restrict information in the system by blocking it for one to access the only information useful to him or her. Have rights from higher ranks to amend/ post anything in the system.
114	Y	8	10	8	10	5	5	5	4	9	10	N	Y	Minimization on access of the system to certain people within the organization especially if it doesn't concern the individual.
115	Y	4	3	4	4	3	5	4	5	8	9	N	Y	Awareness should be done to users so that they know what is required of them.
116	Y	4	2	2	5	5	5	5	3	4	4	N	Y	Setting limits, controls for tasks and processes and ensure checks on them.
117	Y	9	8	7	8	5	5	5	5	8	9	N	Y	Through clear documentation enforcement and revision of laid

														policies as the I.S expands.
118	Y	9	8	8	8	5	5	5	5	8	8	N	Y	
119	Y	7	7	5	6	5	5	5	5	6	5	N	Y	
120	Y	8	8	8	8	5	5	5	5	7	7	N	Y	Form security of password for proper audit trail
121	Y	8	7	8	9	3	3	4	3	7	7	N	Y	
122	Y	9	8	8	9	5	5	5	5	7	10	N	Y	
123	Y	8	8	8	8	5	5	5	4	1	5	N	Y	Training ICT officers
124	Y	10	8	8	8	5	5	5	5	9	9	y	y	
125	Y	6	5	5	5	5	5	2	5	5	3	N	Y	If implemented in all operational areas.

Appendix IV: Zachman's Framework For IS Policy Implementation

	Abstractions (Columns)						
Perspectives (Rows)	**The Zachman Framework**	**DATA What (Things)**	**FUNCTION How (Process)**	**NETWORK Where (Location)**	**PEOPLE Who (People)**	**TIME When (Time)**	**MOTIVATION Why (Motivation)**
	SCOPE (Contextual) Planner	Policies implemented in the list of things important to the business Entity = Class of business things	Defined policies on the list of processes the business performs Function = planning, production and sales	Policies implemented on list of locations in which the business operates note = major business location	Policies implemented on list of organizations important to the business people = major organizations	Policies implemented on list of events significant to the business time = major business event	Policies implemented on list of business goals/strategies ends/means = major business goal/critical Success factor.
	BUSINESS MODEL (Conceptual) Owner	Policies set on the Semantic Model Entity = enablers of IS = Business relationship with service providers	Policies implemented on business process model process = business process I/O = business resources	Policies implemented on business logistics system node = business location link = business linkage	Policies implemented on work flow model people = organization unit work = work product	Policies implemented on master schedule time = business event cycle = business cycle	Policies implemented on business plan end = business objective means = business strategy
	SYSTEM MODEL (Logical) Designer	Policies on Logical Data Model Ent = Data entity, information stored, code, relations = Data relationship	Policies implemented on application architecture process = application function I/O = user views	Policies implemented on distributed system architecture node = IS function, processor and storage	Policies implemented on human interface architecture people = role work = deliverable	Policies implemented on processing structure time = system event cycle = processing cycle	Policies implemented on business rule model end = structural assertion means = action assertion
	TECHNO LOGY MODEL (Physical) Builder	Policies on Physical Data Model Entity= relational data objects	Policies implemented on system design process = computer function I/O = data elements/ sets	Policies implemented on technology architecture node = hardware/ system software link	Policies implemented on presentation architecture people = user work = screen format	Policies implemented on control structure time = execute cycle = Component cycle	Policies implemented on rule design end = condition means = action
	DETAILED REPRESE NTATIONS (Out-of-Context) Sub-Contractor	Data definition entity policies= language syntax	Policies implemented on program process = language statement I/O = control block	Policies implemented on network architecture node = addresses link = protocols	Policies implemented on security architecture people = identity work = job	Policies implemented on timing definition time = interrupt cycle = machine cycle	Policies implemented on rule specification end = sub-condition means = step
	FUNCTIO NING ENTERPRI SE	Policies implemented about actual business data	Policies implemented on actual application code	Policies implemented on actual physical networks	Policies implemented on actual business organization	Policies implemented on actual business schedule	Policies implemented on actual business strategy