American Journal of Computing Research Repository, 2015, Vol. 3, No. 2, 18-27
Available online at http://pubs.sciepub.com/ajcrr/3/2/2

DOI:10.12691/ajcrr-3-2-2

Implementation Framework for Information Systems Policy for Fraud Control in Credit Unions

Samuel Lubanga Oronje*, Christopher A. Moturi

School of Computing and Informatics, University of Nairobi, Nairobi, Kenya
*Corresponding author: samlubanga@gmail.com

Abstract A gap exists in implementing information systems (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 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. A total of 140 questionnaires were distributed out of which 125 were returned and validated. Results demonstrated that low level of implementation of policies leads to high fraud rate and higher chances of future occurrence of fraud. The enforcement level of the policies was 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 Zachman's framework to implement IS policies.

Keywords: *information systems policy implementation, information systems policy framework, savings and credit co-operative societies, credit unions*

Cite This Article: Samuel Lubanga Oronje, and Christopher A. Moturi, "Implementation Framework for Information Systems Policy for Fraud Control in Credit Unions." *American Journal of Computing Research Repository*, vol. 3, no. 2 (2015): 18-27. doi: 10.12691/ajcrr-3-2-2.

1. Introduction

Frequent system changes give attackers an easy way to learn and invade the system [1]. This results to a gap of implementation of IS policies since new users keep joining the system as the old ones leave. As the sensitivity of data changes, the policy has to be re-defined to ensure that it is carefully implemented by all who access 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 Information Systems (IS) policies in place which would sustain implementation of existing policies.

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 [2]. Fraud associated to IS is a problem which prevails within Credit Unions even though there is proof of existing documented policies. 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 [3]. In Kenya there was a draft ICT policy on the website of the Ministry of Information and Communications since February, 2011 for comment [4]. 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.

2. Literature Review

2.1. SACCO Sector

The World Council of Credit Unions statistical report 2013 indicated that there were 57,000 credit unions in 103 countries in 6 continents [5]. The unions contributed USD 1.4 Trillion through savings and shares and had a total worth of USD 1.7 Trillion of asset value. 6,000 of these were located in Kenya contributing USD 2.659 and 4.466 Billion in savings and shares and asset value respectively. SACCOs have great financial contribution to the economy [2]. Based on their asset base, three categories of SACCOs exist: large SACCOs which have assets of over USD 0.04 Billion, a category with only 10; medium SACCOs which have assets between USD 0.01 Billion and USD0.04 Billion, with 41 in this category; small SACCOs, which have assets less than USD. 0.01 Billion and represent the majority with 73 Deposit Taking SACCOs. D.T. 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. The total number of registered and non-registered Credit Unions was more than 6,000 [6]. 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, the national development blueprint. A record total of 48.55% of the National Savings were contributed by this Sector, playing a critical role in the development process in Kenya [7].

2.2. Existing IS Policy Frameworks

The frameworks covered included: Zachman, COBIT, TOGAF, ISO27002 framework, DODAF framework and ITIL framework.

2.2.1. Zachman Framework

This IS architecture framework is depicted as a 6x6 matrix which consists of two independent aspects: rows and columns [8]. 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 United States Department of Veterans Affairs used Zachman's 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.

2.2.2. COBIT Framework

The practicability of COBIT framework in developing control objective has been shown through a model [9]. 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 COBIT's conceptual framework.

2.2.3. TOGAF Framework

TOGAF (The Open Group Architecture) framework was originally designed to support Technology Architecture [10]. 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.

2.2.4. ISO 27002 Framework

The framework 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 [11]. 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 "Command, Control, Communications, Computers, and Intelligence", (C4ISR). Interoperability is one of the key features the framework uses. A "View" model is used that comprise a high level "All View" 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 [12]. However, DODAF does not distinguish views and viewpoints, which significantly complicated their description. As viewpoints, the DODAF's 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

ITIL framework is used as a basis of best practice guidance for IT service management, publications and associated lifecycle phases [13]. 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 members' 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 [14]. However, this study focused on fraud as a challenge within the Credit Unions.

The nature of corporate fraud differs in different surveys, arguments, and media coverage, yet corporate fraud pervasively exists and results to negative consequences. Credit Unions were witnessed to have lost billions of shillings through fraud [15]. There is no organization which is able to completely stop fraud from happening [16]. It has been recognized in previous surveys of fraud that it was only when a fraudster's 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. Sixty-one percent of organizations experienced attempted or actual payments fraud in 2012 [17]. Sixty-seven percent of organizations with annual revenues over USD One Billion were victims of payments fraud compared to half of those with annual revenues fewer than USD One Billion. It implies that unless proper controls are put in place to mitigate fraud, it would be impossible to salvage Credit Unions from collapsing. Credit Unions which were also referred to as Co-operatives; have international guidelines which support a good environment for their development [18]. Fraud on the contrary is not a supportive environment which therefore ought to be controlled.

3. 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. Data Source

The study considered 43 licensed Deposit Taking Credit Unions which were within Nairobi Metropolitan Region in Kenya. 5 respondents from each of the institutions were targeted giving a Population size of 215. There were a total of 215 licensed Credit Unions in the 47 Counties in Kenya. 124 of these were categorized as Deposit Taking Credit Unions [2]. Nairobi Metropolitan Region had 80% of large Credit Unions which were valued at USD 0.04 Billion and above. It also included 60% of medium level which were valued between USD 0.01 to 0.04 Billion and 26% of small Credit Unions, which were valued at less than USD 0.01 Billion.

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 215 employees, the sample size was arrived at as follows:

$$n = \frac{215}{1 + 215*(0.05)^2} = 140.$$

3.3. Data Collection and Analysis

Data collection tools used included questionnaires. 140 questionnaires were administered and were structured such that the respondents remained anonymous. The questionnaire used was divided into three sections namely: Background Information, Level of application of IS and Fraud concerns. A sample of the same is displayed under appendix I. It proved from a study to be a valid and reliable instrument [19]. 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). SPSS version 22.0 software was used for data analysis. Scatter plots, correlation tables and charts were used to present data. Correlations between three variables namely; Implementation_level of IS policy framework, Detected_fraud_level and Potential_fraud_level were examined.

4. Result and Discussion

4.1. Demographic Distribution

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 2 shows background information of the respondents.

Table 1. Credit Unions in Nairobi Metropolitan Region

	Metropolitan region	County	Frequency	%
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

Table 2. Background information of the respondents

			Frequency	%
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 – 3 years	58	46.4
	3	4 – 7 years	18	14.4
	4	8 – 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 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	%	Frequency	%	Frequency	%
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

Table 4. Table of implementation level of IS policy framework

Quantifier	Level weight	% 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

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. 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 1 show a chart of implementation level of IS policy.

Figure 1. Implementation level of IS policy framework

Ten quantifiers were used to measure the level of fraud and are described herein. Identity theft happens when personal detail such login credentials are stolen unlike direct payments fraud which occurs when a fraudster colludes and is paid directly money which was intended for different use. Lapping happens when stolen money from one customer is concealed by replacing the cash from yet again stolen amount from a subsequent customer's payment. Write-offs would occur when a particular debt is considered as a bad-debt leading to cancellation of the account which could be done for manipulative purpose. Diversion of payments happens when money intended for a particular payment is diverted and paid to an individual while payroll and allowances adjustments would happen when claims are filled more than deserved by the beneficiary. Fraudulent financial statements or records include falsifying income statements and manipulation of expenditures and wrong disclosure on financial statements. Frequent changes in accounting estimates is also a fraudulent act done by allowing an entity to have a generally accepted standard different from the original. False documentation is the way fictitious events which never happened are documented and exploiting information pools together aspects of information for easy accessibility by wrong parties.

Table 5 show results from the respondents. 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%. Table 5 show results from the respondents.

Table 5. Table of fraud level

Quantifier	Level weight	% weight
Identity theft	1	10
Direct payments fraud	1	10
Lapping	1	10
Write-offs	1	10
Diversion of payments	1	10
Payroll and allowances adjustments	1	10
Fraudulent financial statements or records	1	10
Frequent changes in accounting estimates	1	10
False documentation	1	10
Exploiting Information	1	10
Total	10	100

Figure 2. Detected fraud level

From Figure 2 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 3 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%. 63% of the respondents pointed out that the fraud level was above 50%.

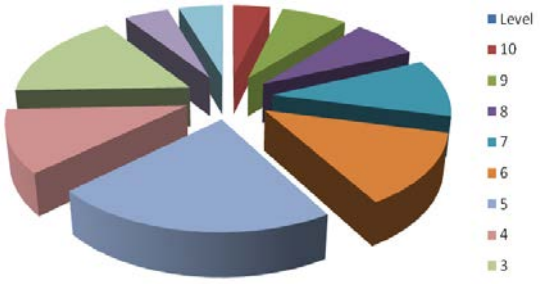

Figure 3. Potential fraud level

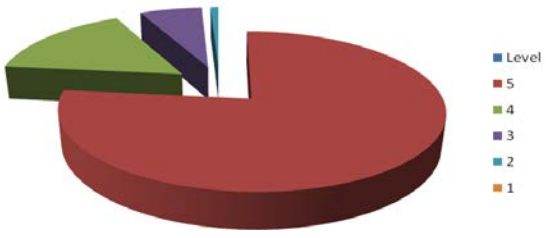

Figure 4. Fraud problem

Table 6. Perceptions concerning fraud

	Fraud problem		Importance of IS policy Framework		Policy Framework use to control fraud		Fraud by employees	
Level	**Frequency**	**%**	**Frequency**	**%**	**Frequency**	**%**	**Frequency**	**%**
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

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.

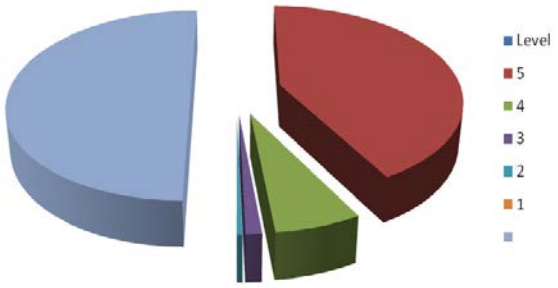

Figure 5. Importance of IS policy framework

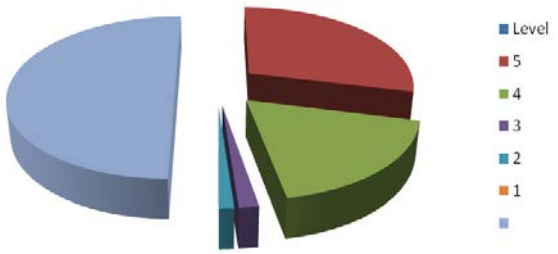

Figure 6. Policy framework use to control fraud

4.2. Data Analysis

Further analysis of the data is as shown in the scatter plot in Figure 7 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).

Correlation of three variables is represented in Table 7.

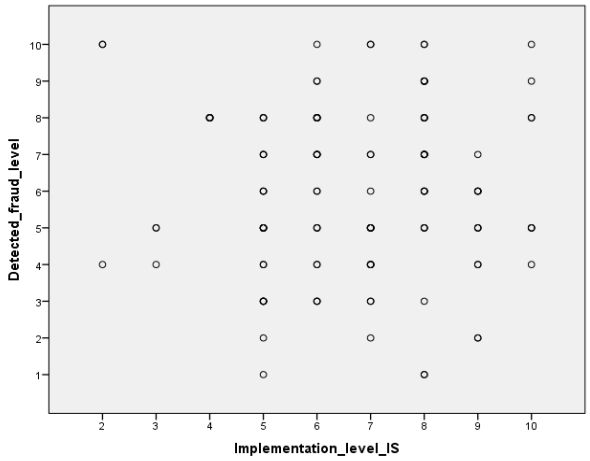

Figure 7. Scatter plot of Detected_fraud_level against Implementation_level of IS policy framework

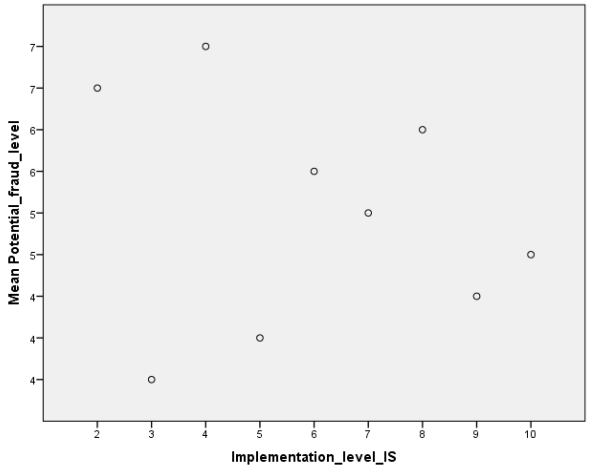

Figure 8. Scatter plot of Potential_fraud_level against Implementation_level of IS policy framework

Table 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 7 showed how two variables namely: Implementation_level of IS and Detected_fraud_level correlated. The Pearson's (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 respondents' 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 Pearson's (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 Zachman's framework.

4.3. Hypothesis Testing

The hypothesis stated that, "Implementation level of IS policy framework has no significant influence on reduction of potential fraud levels in Credit Unions". 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 Pearson's value (r) -0.082 was a negative value. This was equivalent to saying coefficient; $r \neq 0$. Basing on these 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; $r \neq 0$).

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 Zachman's 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). Zachman's 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 [21]. 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 standard's 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 Zachman's 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.

5. Conclusion and Recommendations

5.1. Conclusion

This study resulted to use of the Zachman's framework to implement IS policies. This was achieved by implementing the policies in-line with the 36 matrix elements. 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. Zachman's 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 Zachman's framework also contributes academically for development various areas of study.

5.2. 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.

Acknowledgement

It would not be possible to reach this far without the administration and management of University of Nairobi; which provided an opportunity for the study. We also acknowledge employees of all the Credit Unions who provided data for analysis.

References

[1] Askarov, A. and Chong, S., "Learning is Change in Knowledge: Knowledge-based Security for Dynamic Policies," *Proceedings of the 25th IEEE Computer Security Foundations Symposium (CSF)*, 308-322, June 2012.

[2] SASRA, "SACCO Supervision Annual Report 2012, (Deposit Taking SACCOs)," *SACCO Societies Regulatory Authority (SASRA)*, 2012.

[3] Morgan, J. P., "Association for Financial Professionals," *AFP Payments Fraud and Control Survey Report of Survey results, 2014.* [Online]. Available: http://www.regions.com/virtualdocuments/2014_AFP_Payments_Fraud_Survey.pdf. [Accessed: 15th November 2015].

[4] Waema T, M. and Ndung'u N, M., "Evidence for ICT Policy Action Policy," *Understanding what is happening in ICT in Kenya*, Policy Paper 9, 2012. [Online]. Available: http://www.researchictafrica.net/publications/Evidence_for_ICT_Policy_Action/Policy_Paper_9_-_Understanding_what_is_happening_in_ICT_in_Kenya.pdf. [Accessed: 15th November 2015].

[5] World Council of Credit Unions, 2014. [Online]. Available: http://www.woccu.org/. [Accessed: 19th November 2015].

[6] SASRA, "SACCO Supervision Annual Report 2013, (Deposit Taking SACCOs)," *SACCO Societies Regulatory Authority (SASRA)*, 2013.

[7] Kenya Economic Report, "*Creating an Enabling Environment for Stimulating Investment for Competitive and Sustainable Counties,"* Kenya Institute for Public Policy Research and Analysis, (KIPPRA), 2013.

[8] Radwan, A. and Aarabi, M., "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, 22-24, January 2011.

[9] Zhang, S., and Le, F. H., "An Examination of the Practicability of COBIT Framework and the Proposal of a COBIT-BSC Model," *Journal of Economics, Business and Management*, 1(4). 391-395.

[10] The Open Group [Online]. Available: http://www.opengroup.org/standardsprocess/Standards_Process-Overview.pdf. [Accessed: 21st November, 2015.

[11] ISO, International Standard (ISO/IEC27002), "*Information technology - Security techniques - Code of practice for information security controls,"* Switzerland, 2013.

[12] Cameron, B. H., and Mcmillan, E., "Analyzing the Current Trends in Enterprise Architecture Frameworks," *Journal of Enterprise Architecture*, 60-71 February 2013. [Online] Available: http://ea.ist.psu.edu/documents/journal_feb2013_cameron_2.pdf [Accessed: 22nd November, 2015].

[13] Brooks, P., "Metrics for Service Management," *Designing for ITIL*, Van Haren, Zalbommel, 2012.

[14] Wanyama F.O., "Surviving Liberalization," *The Co-operative Movement in Kenya*, International Labour Organization, Coop Africa Working Paper No.10, 2009. [Online] Available: http://ilo.org/public/english/employment/ent/coop/africa/download/wp10_survivingliberazation.pdf [Accessed: 22nd November 2015].

[15] Lin, C., Song, F. M. and Sun, Z., "*The Financial Implications of Corporate Fraud,"* 2011. [Online] Available: http://www.fin.ntu.edu.tw/~conference/conference2012/proceedings/files/A193_Financial%20implications%20of%20fraud_Nov_01.pdf [Accessed: 22nd November 2015].

[16] Warfield, B., "*Employee Fraud in Australian Credit Unions*, 2013. [Online] Available: http://www.warfield.com.au/Warfield%20Fraud%20Report%202013_HQ.pdf [Accessed: 22nd November 2015].

[17] Morgan, J. P., "Association for Financial Professionals," *AFP Payments Fraud and Control Survey Report of Survey Results*, 2013. [Online]. Available: http://www.larutech.com/jan2014/2013_AFP_Payments_Fraud_Survey.pdf. [Accessed: 22nd November 2015].

[18] Munkner, H-H., "Worldwide regulation of co-operative societies – an Overview," *European Research Institute on Cooperative and Social Enterprises Working Paper*, 53 (3). 2013. [Online] Available: http://euricse.eu/sites/euricse.eu/files/db_uploads/documents/1371044429_n2351.pdf [Accessed: 27th November 2014].

[19] Polikandrioti, M., Goudevenos, I., Michalis, L., Nikolaou, V., Dilanas, C., Olympios, C., Votteas, V., and Elisaf, M., "Validation and reliability analysis of the questionnaire: Needs of hospitalized patients with coronary artery disease," *Health Science Journal*, 5 (2). 137-148. 2011.

[20] United States. National Institute of Standards and Technology. "*Trend Micro Products (Deep Security and Secure Cloud),"* 2012 [Online] Available:

http://www.trendmicro.com/cloud-content/us/pdfs/business /oth_fisma-nist-solution-profile.pdf. [Accessed: 27th November 2014].

[21] Witherell, P., Rachuri, S., Narayanan, A., Lee, J.H., *FACTS: A Framework for Analysis, Comparison, and Testing of Standards.* U.S. Department of Commerce: National Institute of Standards and Technology, 2013 [Online] Available: http://nvlpubs. nist.gov/nistpubs/ir/2013/NIST.IR.7935.pdf [Accessed: 26th November 2015].

Appendices

Appendix I: Structured Questionnaire

This study is 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 (√) 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 (√) 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 (√).

		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 (√) 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 (√) 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: 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 ENTERPRISE	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