International Journal of Advanced Engineering and Technology
ISSN: 2456-7655; Impact Factor: RJIF 5.54
Received: 23-03-2020; Accepted: 02-04-2020; Published: 22-04-2020
www.newengineeringjournal.com
Volume 4; Issue 2; 2020; Page No. 01-07

An empirical investigation of the adequacy of security controls of computerized accounting information systems (CAIS) in the listed companies in Zambia

Frank Munthali[1], Victor Muchemwa[2], William Phiri[3], Euphrasia Ng'andwe[4]
[1] Zambia Cooperative Federation, Zambia
[2] University of Zambia, Institute of Distance Education, Zambia
[3] Chalimbana University, Department of Information and Communications Technology, Zambia
[4] Chalimbana University, Library, Zambia

Abstract
The rapid development of IT, availability of user-friendly accounting software and the increased competition have forced companies to adapt CAIS in order to remain competitive whereas threats to CAIS are unavoidable in the dynamic environment. In this scenario, security controls of CAIS are vital to any organization. This study examined the existence and adequacy of implemented computerized accounting information system (CAIS) security controls to prevent, detect and correct security breaches in listed companies in Zambia. An empirical survey using a self-administered questionnaire was carried out to achieve the objective. The results of the study spotlight a number of inadequately implemented CAIS security controls and significant differences among listed companies regarding the adequacy of implemented CAIS security controls. Based on the findings, some recommendations are given to strengthen the breaches in the present CAIS security controls in the listed companies. Findings of this study will help accountants, auditors, managers, and IT users to better understand and secure their CAIS in order to achieve success of their visions.

Keywords: accounting, computer security control, information systems

1. Introduction

1.1 Background of the Research

Information is now being considered as one of the most valuable assets for most organizations. This is attributed to the fact that business survival and success are heavily dependent upon the accuracy, integrity and continued availability of critical information. Ismael and King (2007). The reliance on information and continuous changes in technology, force organizations to implement security controls to protect their Computerized Accounting Information Systems (CAIS) against potential security threats. However, the failure to secure the CAIS and the information they contain or to make it available when it is required can, and does, lead to great financial and non-financial losses. It is argued that individuals who are more aware of the potential security threats against their CAIS would be more sensitized to the dangers of inadequate security controls and would more likely feel that their CAIS security is unsatisfactory.

Computers have enabled accounting tasks to be accomplished much faster and more accurately whereas threats to computerized accounting information system (CAIS) are unavoidable in the dynamic IT environment. IT, in many cases, has been developed faster than the advancement in security control practices and has not been combined with similar development of the employees' knowledge, skills, awareness, and compliance. Implementing adequate security controls and its related facilities used in handling, recording, processing, storing and distributing information has become a necessity (Smith, 2016) [12].

Many organizations do not realize the importance of CAIS security until some unauthorized access to their systems occurs or modification, alteration or destruction of their critical files has happened. Organizations can no longer disregard the importance of information security in the light of computer fraud, hackers and computer viruses. Accordingly, the need to understand and employ adequate security controls over CAIS has become an issue no business can ignore.

The great desire to automate business processes in Zambia has made organizations to acquire and implement systems and software which could come in form of turnkey systems (e.g. generalized accounting systems, special-purpose systems, and office automation systems); backbone systems; vendor-supported systems; and Enterprise Resource Planning (ERP) systems. The trend of technology has promoted the sophistication of these commercial packages away from construction and delivery of in-house packages.

Essentially, the application of software to accounting has been further engendered by the growth of commercial software market which have relatively low cost as compared to customized software; emergence of industry-specific vendors who targets their software to the needs of particular types of businesses; growing demand for software by businesses; and the trend toward downsizing of organizational units and the resulting move toward distributed data processing environment, which has made commercial software options more appealing to larger organizations especially those listed on Lusaka Stock Exchange (LUSE) in Zambia.

The advent of the Information Technology (IT)-led era, availability of user-friendly accounting software and the increased competition have forced companies to adapt to CAIS in order to remain competitive. In Zambia, the number of listed companies on LUSE has steadily increased over the past years. The listed companies now on LUSE stand at 22 (Twenty-two) as at 2018 (Munthali, 2010) [11]. Research findings show that many companies listed on Lusaka Stock Exchange, such as Lafarge Cement PLC, Zambia Sugar PLC, Standard Chartered Bank PLC, Investrust Bank PLC, Madison Financial Services PLC, Zambia Breweries PLC, National Breweries PLC, Zambia National Commercial Bank PLC, Airtel PLC and many more are computerized to do their accounting activities. The listed companies have used either one of the following software packages to get their desired accounting software packages. Tailor made accounting software package: Develop accounting software package as per their requirements or Purchase one of the software packages from the market (e.g. Acc Pac, Quick Books and so on).

1.2 Statement of the Problem

Studies have shown that most listed companies in Zambia implement CAIS security controls. However, it has not been established whether the Computer Accounting Security Controls are adequate to prevent security threats from occurring. Hence the need to undertake a study to establish the adequacy of CAIS in the listed companies in Zambia.

1.3 Objectives of the Study

To investigate the adequacy of implemented CAIS security controls in Listed Companies in Zambia, in order to prevent, detect and correct CAIS security breaches

1.4 Research Questions

Are the security controls implemented in the Listed Companies in Zambia adequate?

1.5 Conceptual Framework

According to Metrejean, Smith, and Elam (2005) [9] the extent and impact of security controls of CAIS in Listed Companies depends on various factors such as; business type of listed Company, size of the Company, qualifications of staff, level of experience with CAIS, training on security controls of CAIS, level of awareness of security controls of CAIS among staff, availability of resources, availability of security policy and conducive working environment.

In addition, the positive impact of adoption of security controls of CAIS includes; protection of computerized information, prevention of fraud by employees within the organization, prevention of unauthorized access to Computerized Accounting Information Systems and transactions will be easily traceable. However, need for additional training of staff and additional costs are some of the challenges of establishing security controls CAIS.

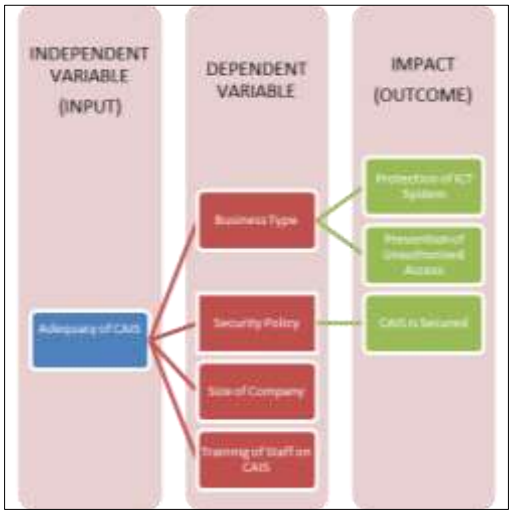


Fig 1: Conceptual Framework

2. Literature Review

According to Kennedy, (2015) [5] Computerized Accounting Information Systems (CAIS) are becoming more willingly available to all types and size of licensed banks. This is as a result of the increase in growth and real time online data processing in CAIS which has made access to these systems supplementary available and easier for many users in addition to a rapid increase in volume of banking transactions. As a result, computerized accounting frauds are also escalating. He further reveals that erasing customer data base, planting a dangerous virus, rifling through corresponding files, sending Trojan horse, personnel records and searching for active credit card numbers, system hacking frauds, network frauds and password frauds are just a few of attacks that may be directed at the victim's CAIS. As such all the licensed banks need to be aware with the potential security threats that might challenge their CAIS and implement the relevant security controls like access controls, division of responsibilities, continuous changes in user passwords, output security controls, offline programs and data security to prevent, detect and correct such security breaches.

In another study, Kennedy (2013) [6] carried out an Empirical Investigation of the Security Controls of Computerized Accounting Information Systems (CAIS) in the Selected Listed Companies in Sri Lanka and the significant differences among the listed companies regarding the above research issue. The findings revealed weak security controls of CAIS. Although results from one sample t test revealed all the implemented CAIS security controls were at adequate level. The following CAIS security controls – security policy, hardware and physical access security controls, software and electronic access security controls, data security controls, separation of duties, output security controls and SCCPA fell into categories of adequate and good/higher level of security controls and rest of the CAIS security controls fell into categories of poor and adequate level.

The study reported that CAIS security controls such as administrative security controls, data security controls, offline programs and data security controls, utilities security controls, bypassing of normal access security controls and output security controls, it was discovered that there were significant differences among the listed companies regarding the adequacy of implemented CAIS security controls. Therefore, there was need for prompt attention to be given in all areas of the security controls of CAIS.

Malami *et al*. (2012) [10] explored threats to CAIS in their study on "Security Threats of Computerized Banking Systems (CBS): The Managers' Perception in Malaysia." They revealed that the major threats challenging the Computerized Accounting Information Systems of banks in Malaysia included human intentional threats, technological threats, environmental threats, and natural threats. While findings from the study conducted by Abu-Musa (2004) [1] on Security Controls of CAIS in an Emerging Economy in Egypt established that the computer departments paid relatively more attention to technical security controls (such as: software and electronic access security controls, data and data entry security controls, off-line programs and data security controls, utility security controls, bypassing security controls, and user programming security controls); while internal audit departments emphasized the behavioral and organizational security controls (e.g. organizational security controls, division of duties, and output security controls). The study provided invaluable empirical results regarding inadequacies of implemented CAIS security controls, and made some suggestions to strengthen the security controls in the EBS.

However, Loudon and Loudon (2016) established that the major threats to CAIS are internal employees. They pointed out that organizations tend to think the security threats to a business originate outside the organization. They argued that company insiders posed serious security problems. They attribute this to the fact that employees have access to privileged information, and in the presence of sloppy internal security procedures, they are often able to roam throughout an organization's systems without leaving a trace. Other studies have also found that users' lack of knowledge is the single greatest cause of network security breaches. Many employees forget their passwords to access computer systems or allow co-workers to use them, which compromises the system. Malicious intrudes seeking system access sometimes trick employees into revealing their passwords by pretending to be legitimate members of the company in need of information. This practice is called social engineering. Both end users and information systems specialists are also a major source of errors entering faulty data or by not following the proper instructions for processing data and using computer equipment. Malami *et al*. (2012) [10], in their study which investigated "Internal Human based Threats and security Controls in Computerized Banking Systems", in Malaysia seem to agree with this assertion and established that lack of technical and/or adequate knowledge among the employees to operate the system posed as a threat to the security controls in banks.

They recommended that continual training of employees should be scheduled and computer system and/or robot system should be put in place to substitute human services. In addition, prior studies (Loch *et al*., 1992; Neumann, 1995; Baskerville, 1996; Cohen, 1997) confirmed that human unintentional threats were the most significant threats against the information system. However, Paul and Baskerville (2005) longitudinal study of information system threat contradicted prior studies that human unintentional errors were the major threats to information system. Their results indicated that the threats appeared to be insignificant and a poorly recognized issue for information systems security. In addition, the result of their study was also inconsistent with this current study as the findings of this current study indicated high level of the likelihood of this threat the study concluded.

As observed by Chalwe, (2017) [3] in the study on "Technology and its impact on the Accountancy Profession" most business organizations especially banks, in Zambia which have Implemented Computerized Accounting Information Systems have been victims of fraud by Fraudsters due to inadequate computer security controls. He advised that organizations especially banks and big listed companies using (CAIS) must put in place robust IT security controls like security policies, rotation of duties, training of staff in security controls, access security, encryption of data during transmission, data security controls and periodic changes to the passwords in use to prevent fraudulent activities.

There seems to be enough evidence that there are higher possibilities of threats to CAIS. These types of threats are prevailing in the developed as well as the developing countries. They seem to be present in all types of organizations without size differences including those listed Zambia Stock Exchange. However, there is need to probe further on this subject in order to establish how adequate security controls implemented in these companies are in order to validate the assumption.

3. Methodology

An empirical survey – using a self-administered questionnaire was conducted to investigate and evaluate the existence and adequacy of implemented CAIS security controls in all Listed Companies. The questionnaire used five-point Likert Scale (perfect, good, adequate, poor, not at all) questions/ statements to make it easy for respondents to answer these questions/ statements and to go through the questionnaire. The population of this study comprised of Listed Companies on Lusaka Stock Exchange (LUSE). Sample framework comprised of 22 companies including; (4) Mining related Companies, (8) Manufacturing, (7) Banking, Financing and Insurance, (1) Hospitality and (2) Telecoms and Energy. Data collected was analyzed using Statistical Package for Social Sciences (SPSS) version 20. Descriptive statistics (such as frequencies and percentages) of data was performed to identify the main characteristics of the research variables. One sample t test was used to test adequacy of the implemented CAIS security controls in the listed companies.

Adequacy of CAIS Security Control was = $\mu \geq 3$

Where μ is the mean of security controls. Overall security controls were obtained by aggregating 11 types of security controls.

Statistical format of above hypothesis (1) was as follows, H10. $\mu \leq 2.99$ H1A. $\mu > 2.99$

Determine whether reject the null hypothesis or not. The decision rule was:

If the one-tailed critical t value was less than the observed t, then H0 is rejected.

Make decision about null hypothesis based on:

- Probability of F-statistic ≤ 0.05 a reject null hypothesis
- Probability of F-statistic > 0.05 a fail to reject null

hypothesis

One-way ANOVA was used to test the significant differences among the listed companies regarding the adequacy of implemented CAIS security controls.

The external reliability of the instrument used to collect data was examined by Test – Retest method. This test was carried out by using 12 companies from different sectors with three weeks' time interval. The coefficient of the Test – Retest of the instrument indicated a high external reliability 0.932 (correlation is significant at the 0.01 level -2 tailed). The inter item consistency reliability was examined with Cronbach's Alpha test. The result of Cronbach's Alpha test was 0.926 which suggested that the internal reliability of instrument was very high.

Content validity of the instrument was ensured by the conceptualization and operationalization of the variables based on literature, and indirectly by the high internal consistency reliability of the instrument as denoted by alphas.

4. Findings and Discussion.

4.1 Business Type

The table below shows the population, sample size and responses that were obtained in order to establish the type of businesses and population size;

Table 1: Research Sample – Business Type

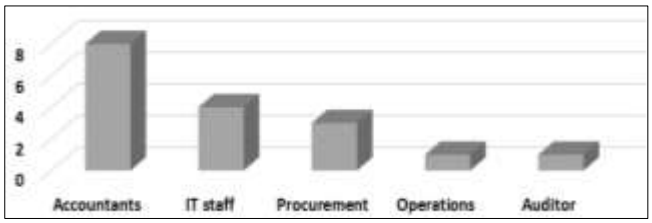
Category	Population	Sample size	Collected	
			Number	Percentage
Mining and Construction	4	4	3	75%
Manufacturing	8	8	6	75%
Bank, Finance and Insurance	7	7	6	86%
Hospitality	1	1	1	100%
Telecommunication and Energy	2	2	1	50%
Totals	22	22	17	

***Source*:** (Field Data, 2016)

The findings show that the study obtained a (17/22) (77%) response rate from the distributed questionnaires. Mining and Construction, Manufacturing, Bank, Finance and Insurance, Hospitality and Telecommunications and Energy include the type of businesses that were selected for this study. Basically therefore, this implies that majority of the population sampled participated successfully giving us grounds to make generalizations on the subject.

4.2 Respondent's job titles

The respondents from the selected companies who participated in this study comprised of (8) Accountants, (4) ICT Staff, 3 Procurement, (1) Operations and (1) Auditors as shown in the table below;



***Source*:** Field Data, 2019

Fig 2: Respondent's job titles

Based on the conceptual framework presented in the preceding text, staff training was identified as an independent variable impacting positively on the adequacy of CAIS. Based on this fact, respondents were asked to indicate their general professions so that a link could be drawn on how adequate CAIS was being implemented based on the levels of staff qualifications.

4.3 Security Policy

The study sought to explore the existence and the implementation of adequate security policy in the listed companies, the respondents were requested to answer to relevant security policy questions. As indicated by mean values in the Table 3. 2 below, the implemented Security Policies were found to be above adequate level at 4 and above and approaching higher security level regarding all aspects of security policies in the listed companies. Information security policy document was good or higher level in the majority of listed companies that can be assured based on mean, median, mode.

The critical t (d. f 16, α=0.05) is 1.746 and the observed t value was 3.529,

H1(i) 0 is rejected and H1 (i) A is accepted at 5% significant level. That is, there was sufficient evidence to conclude that the mean number of Security Policy is greater than 2.99 and implemented Security Policies of CAIS in the listed Companies are adequate.

Test of Homogeneity of variances, revealed the significance was 0.090, which was greater than 0.050. So, the variances were approximately equal for the Security Policy.

ANOVA at 0.0380 significance, it means there are significant differences among the listed groups companies regarding the existence and implementation of the security policy of CAIS at significance level of 0.05. The mean of Bank, Finance and Insurance Companies are significantly different from other sectors for Administrative Security Controls.

Table 2: Security Policy

Security Policy	Mean	Std. dev.	Median	Mode
1. Information security policy document is in place	4.24	1.348	5.00	5
2. Review of information security policies	4.00	1.323	4.00	5
3. Coordination with other security policies	4.12	1.317	5.00	5

***Source*:** Field Data (2016)

4.4 Administrative security controls

According to the findings, Administrative Security Controls were above adequate level in the listed companies. The positive Management attitude towards the security of CAIS had the highest mean of 4.59 with a very low standard deviation of 0.618 indicating consistency of the mean

towards the actual values.

This result shows a positive acceptance and confidence by administrators to implement and manage the CAIS security model. More than 50% of companies reported that rotation of duties helped to identify the errors and irregularities. The mean for rotation of duties in most listed companies was at good or higher level which was assured by median and mode. However, the lowest mean 3.06 was the bonding of employees who had access to sensitive data, and a standard deviation of 1.478. The rest of the factors like Mandatory vacation used to reduce the fraud resulting from increased chance of exposure, Personnel policies included, background checks to reduce the hiring dishonest employees, there was documentation showing that users were properly trained, with a mean ranging from 3 to 4 which was positive.

The critical t was 1.746 and the observed t is 4.809, there was sufficient evidence to conclude that the mean number of Administrative Security Controls is larger than 2.99 and the implemented Administrative Security Controls of CAIS in the listed companies were adequate.

Test of Homogeneity of variances revealed the significance was 0.775, which was greater than 0.050. Therefore, the variances were approximately equal for Administrative Security Controls.

ANOVA was calculated at 0.194 revealed there were no significant differences among the listed companies regarding the existence and the implementation of the Administrative Security Controls of CAIS at significance level 0.05.

3.5 Hardware and physical Access Security Controls

The mean value of implemented theft and hazard insurance covering computers' hardware, limiting computer access to employees with a defined need, protection of computers from water, smoking and dust, restriction of physical access to terminals, computer room, hardware outside the computer room (e.g. network switch-gear, modems), communication lines (e.g. cables should be sealed in ducts outside the hardware area to prevent tapping or reading by service equipment) was around 4 and fell under the higher and perfect level.

The median values also showed that more than 50% of respondents had higher security controls over the generating and revoking the means of permitting physical access (e.g. key, security badge, combination number, switch card) and the person responsible for controlling physical access was independent of programming, system software, and accounting control functions while rest of them fall into categories of adequate and good level.

On contrast, the mean of installing alarms and video camera in areas with high concentration of computer equipment was 2.88 and standard deviation was also high at (1.799). Therefore, it was noted that several (10) responded companies representing 59% were poor and not at all level in relation to implemented installing alarms and video cameras in high concentration of computer equipment areas.

The critical t was 1.746 and the calculated t was 9.147, there was sufficient evidence to concluded that the mean number of Hardware and Physical Access Security Controls was larger than 2.99 and the implemented hardware and physical access security controls of CAIS in the listed companies were therefore adequate.

Test of Homogeneity of variances, revealed the significance was 0.865, which was greater than 0.050. Therefore, the variances were approximately equal for hardware and physical Access Security Controls.

The ANOVA test at 0.861 showed that there were no significant differences among the listed companies regarding the existence and the implementation of the Hardware and Physical Access Security Controls of CAIS at significance level of 0.05.

4.6 Utilities Security Controls

The statistical Table 4.8 shows that three (3) of the four (4) aspects of implemented utility program were above the adequate level of 3, but standard deviation of utility program was above 1.

This means that a lot of companies fall between the poor and good level. More than 50 % of the companies mentioned that implemented procedures to identity such program and implemented security controls to log and report the use, or attempted use, of such programs were below the mean of 3 and stand deviation of 2.88. 41% of respondents reported the ability to use such programs needed to be adequately restricted to appropriate, authorized personnel in the Listed Companies.

While the critical t was 1.746, the observed t was 0.588 implying that there was no sufficient evidence to conclude that the mean number of Utilities Security Controls is larger than 2.99 and therefore, the implemented Utilities Security Controls of CAIS in the listed companies were not adequate**.**

Test of Homogeneity of variances revealed the significance was 0.686, which was greater than 0.050. As such, the variances were approximately equal for Utilities Security Controls.

The ANOVA was at 0.109. It can therefore be stated that there were no significant differences among the listed companies regarding the existence and implementation of the Utilities Security Controls of CAIS at the significance level of 0.05.

Table 3: Utilities Security Controls

	Mean	Std. dev.	Median	Mode
1. When or other special programs could be used to change application programs/data by bypassing normal software access restrictions: 1. Procedures should be implemented to identify all programs with this special status	3.00	1.768	3.00	1
2. The ability to use such programs should be restricted to appropriate, authorized personnel in the organization	3.12	1.833	3.00	5
3. Security controls to log and report the use or attempted use, of such programs should be implemented.	2.88	1.453	3.00	3
4. A review of such reports should be performed by a responsible official to determine and investigate unauthorized access.	3.18	1.629	3.00	5

***Source*:** Field Data (2016)

4.7 Output Security Controls

According to the findings presented in Table 4.7 below, the mean values of the following security controls was at 4 and above. Visual access to sensitive information is controlled and restricted only to the authorized users in the authorized time, Printing and distribution of data and information is under proper security controls, and only by

authorized persons in the organization and Shredding (cutting) machines are available and used for disposal of confidential data.

Printing of sensitive data outside and data center or central computer room and sensitive computer output secured in a locked cabinet was at the mean 3 and above which was an indication of a higher level of output of security controls.

Mean and standard deviation of hard copy output automatically date and time stamped were at a mean of 2.63 and 1.310 respectively and this security control fell between poor and not at all level. 53% of the companies responded that they did not have this control in place.

On the other hand, most of the responded companies indicated that usefulness of shredding machines in their company for disposal of confidential and sensitive data is between good and adequate level. It is proved by values of mean (4) and above and standard deviation of (0.903).

The critical t is 1.746 and the observed t is 4.303, which is an indication of sufficient evidence to conclude that the mean number of output security controls is larger than 2.99 and the implemented output security controls of CAIS in the listed companies were adequate.

Test of Homogeneity of variances in**,** reveals the significance is 0.917, which is greater than 0.050. So, the variances are approximately equal for Output Security Controls.

The ANOVA was calculated at 0.692 indicating no significant differences among the listed companies regarding the existence and the implementation of the output security controls of CAIS at Alpha=0.005.

Table 4: Output Security Controls

	Mean	Std. dev.	Median	Mode
1. Visual access to sensitive information should be controlled and restricted only to the authorized users in the authorized time	4.06	0.899	4.00	5
2. Printing of sensitive data outside the data Centre or central computer room should be under security controls	3.41	0.870	3.00	3
3. Sensitive computer output should be secured in a locked cabinet	3.35	1.539	4.00	5
4. Hard copy output should be automatically date/time stamped	2.63	1.310	3.00	3
5. Security controls should be implemented over printed copies of data/information	3.88	1.111	4.00	5
6. Printing and distribution of data and information done should be under proper security controls, and only by authorized persons in the organization	4.18	0.883	4.00	5
7. Shredding (cutting) machines should be available and used for disposal of confidential data	4.24	0.903	5.00	5
8. Shredding of sensitive documents should be restricted to security cleared personnel	3.41	1.543	4.00	5

***Source*:** Field Data:2019

5.0 Conclusion

The study established that there were differences among the listed companies regarding Computerized Accounting Information Systems in the listed companies in Zambia. This is in addition to weak security controls of CAIS. Results of one sample t test revealed that out of 11 listed security controls, 6 of them representing 55%, had adequate CAIS security controls while 45% of them were inadequate and ranged from poor to adequate level.

However, the following CAIS security controls; security policy, hardware and physical access security controls, software and electronic access security controls, output security controls and SCCPA fell into categories of adequate and good/higher level of security controls and rest like data security controls, utilities security controls, separation of duties and by passing of normal access security controls of the CAIS fell into categories of poor and adequate levels.

Furthermore, the outcomes of the study spotlight a number of inadequately implemented elements of CAIS security controls. The study reported following CAIS security controls such as administrative security controls, data security controls, utilities security controls, and output security controls had significant differences among the listed companies regarding the adequacy of implemented CAIS security controls.

"If there is a small hole on the tube which is filled with air the entire air will be deflated. Similarly, if there is any small weakness in the security controls of CAIS, the company may lose," therefore, prompt attention should be given in all areas of the security controls of CAIS.

6.0 Recommendations

The study recommends are the following in order to eliminate weaknesses and strengthen the implemented CAIS security controls for short and long terms in listed companies.

6.1 Short term

6.1.1 Security policy: It is important to implement information security properly and take necessary legal action when any one misuses the information system.

6.1.2 Administrative security controls: Adequate steps should be taken to restrict access to companies' sensitive data to the authorized employees with defined needs. Make an agreement with employees who have deal with sensitive data. Introduce rotation of duties to identify the errors and irregularities.

6.1.3 Hardware and physical access security controls: Companies are recommended to install video cameras in areas with a high concentration of computer equipment. Increase the security of computer when not in use. Complete independence of individuals who are responsible for controlling physical access and those who are responsible for programming, system software, and accounting control functions should be considered.

6.1.4 Software and electronic access security controls: Security controls of mobile computing and teleworking will be increased by the companies which deal with mobile computing and teleworking. Implement up to date technology to prevent unauthorized public access to the companies' accounting information systems via dial-up (for example, by use of dial-back, and by dial-up access restricted to non-confidential information). It is valuable to extend current insurance to cover software too. Further, Software backups, like originals, should have write protect tabs in place.

6.1.5 Data security controls: Sensitive data stored off-site should be encrypted to reduce the chance of its unauthorized exposure. Prepare and implement emergency plan should

state the main steps that should be taken when systems fail and who is responsible for completion of the steps in listed companies.

6.1.6 Off-line programs and data security controls: Increase the security control on programs and data, including back-up copies are physically controlled such as storage methods should prevent the unauthorized removal of programs/data (e.g. diskettes/ flash drive) and security controls should be implemented over issuing and returning of programs/data files. The librarian functions should be performed by individuals who are entirely independent of computer operation and programming responsibilities.

6.1.7 Utilities security controls: More attention should be directed by listed companies to strengthen utility security controls to identify all utility programs or other special programs and to implement adequate security controls over the use, or even attempts at use, of such programs.

6.1.8 Output security controls: Companies should introduce shredding (cutting) machines for disposal of confidential data and shredding of sensitive documents should be restricted to security cleared personnel. Most output security controls were at higher level but they should take more actions on what was mentioned in the questionnaire under the output security controls to reach perfect level.

6.2 Long term measures

6.2.1 Security policy: The information security policy or policies should be reviewed at planned intervals, and when significant changes in the external environment occur, to ensure its continued suitability, adequacy and effectiveness.

6.2.2 Administrative security controls: Companies which do not have background check to select the employees should include background check to reject the dishonest employees. Mandatory vacations of employees should be taken where not already implemented.

6.2.3 Hardware and physical access security controls: As for physical entry control - Secure areas should be protected by appropriate entry controls to ensure that only authorized personnel are allowed access such as authentication mechanisms (e.g., keycard and PIN) proportionate to the identified risks and the value of the asset(s) protected.

6.2.7 Utilities Security controls: A review of such reports should be performed by a responsible official to determine and investigate unauthorized access, the ability to use such programs should be restricted to appropriate, authorized personnel in the organizations.

6.2.8 Output security controls: Hard copy output should be automatically date/time stamped for easy identification. Printing of sensitive data outside the data center or central computer room should be under security supervision. Sensitive computer output should be secured in a locked cabinet. Security controls should be implemented over printed copies of data/information for example keeping of record of printed documents. 6.Printing and distribution of data and information done should be under proper security controls, and only by authorized senior management persons in the listed companies.

6.2.9 Security controls of correct processing in applications: Control of internal processing- validation checks should be incorporated into applications to detect the corruption of information through processing errors or deliberate acts. Output data validation – Random output/input comparisons should be regularly done to verify correct processing.

7. References

1. ABU-MUSA AA. Investigating the Security Controls of CAIS in an Emerging Economy: An Empirical Study on Egyptian Banking Industry: The Journal of Managerial Auditing. UK. 2004c; 19(2):272-302.
2. Byemba E. ICT Profile for Zambia: A brief summary of ICT development in Zambia, 2010, P. 1-4.
3. Chalwe A. Annual Business Conference (ABC): Technology and its impact on the Accountancy Profession: Livingstone Zambia. Wednesday 16th August to Friday 18th 2017. ABC Secretariat, 2017, p. (8).
4. Ismail NA, King M. The factors influencing the alignment of Accounting Information systems in small and medium Malaysian manufacturing firms: European Scientific Journal December 2013 /SPECIAL/ edition, 2007, 1. ISSN: 1857 – 7881 (Print) e - ISSN 1857- 7431
5. Kennedy GD. An Empirical Investigation of the Security Controls of Computerized Accounting Information Systems (CAIS) in the Selected Listed Companies in Sri Lanka, 2013. Available [online] at
6. Kennedy GD. An Empirical Investigation of the Computerized Accounting Information Systems Frauds in Licensed Banks in Sri Lanka: [Online], 2015. Available at SSRN: https://ssrn.com/abstract=2932007. [Accessed Oct.2017]
7. Kothari CK. Research Methodology, Methods and Techniques: Willey Eastern Ltd, New York, 2006.
8. Laudon KC, Laudon JP. Management Information Systems: Managing the Digital Firm.14th Edition-Global Edition, Edinburgh Gate, Harlow, England: Pearson Education Publishers, 2016, p. 335-375.
9. Metrejean E, Smith HG, Elam D. Educating accounting students on computer crime and ethics: Journal of business and economic research. 2005; 3(9):77-88.
10. Malami A, Zainol Z, Nelson S. Security Threats of Computerized Banking Systems (CBS): The Managers' Perception in Malaysia: International Journal of Economics and Finance Studies. 2012; 4(1):21-30.
11. Munthali GF. Effectiveness of implemented data security controls at the Zambia Transport Information Systems (ZAMTIS) of the Road Transport and Safety Agency (RTSA): An Empirical study: MBA, Eastern and Southern Africa Management Institute (ESAMI), Nov, 2010, P. 38-43.
12. Smith JS. Accounting Information Systems: Ethics, Fraudulent Behavior, and Preventative Measures. University Honors Program Theses, 2016, 178.
13. Talal H, Hayale HA, Khadra A. Evaluation of The Effectiveness of Control Systems in Computerized Accounting Information Systems: An Empirical Research Applied on Jordanian Banking Sector. Journal of Accounting – Business & Management. 2006; 13:39-68.