AN EMPIRICAL INVESTIGATION OF THE SECURITY CONTROLS OF COMPUTERIZED ACCOUNTING INFORMATION SYSTEMS (CAIS) IN THE SELECTED LISTED COMPANIES IN SRI LANKA

Rajeshwaran N. [1]
Gunawardana K. D.[2]

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 the organizations. This study examines the existence and adequacy of implemented computerized accounting information system (CAIS) security controls to prevent, detect and correct security breaches in the selected listed companies in Sri Lanka. An empirical survey using a self-administered questionnaire has been carried out to achieve the objective. 41 out of 118 usable questionnaires have been collected to different types o cais f companies representing 13 out of 20 sectors from 4th November to 10th December 2008. 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 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, Information Technology

1. BACKGROUND TO THE STUDY

The advent of the IT-led era, availability of user friendly accounting software and the increased competition have forced companies to adapt CAIS in order to remain competitive. Computer has also enabled accounting tasks to be accomplished much faster and more accurately whereas threats to computerized accounting information system (CAIS) are unavoidable in the dynamic environment.

Many companies such as Abans Electricals Limited, Asiri Surgical Hospital PLC, Ohn Keells Hotels PLC, Hatton National Bank PLC, Hemas Holdings PLC, Balangoda Plantations PLC, Dialog Telekom PLC, etc. are computerized to do their accounting activities. One of two ways has been used by them to get their desired accounting software package.

1. Tailor made accounting software package: Develop accounting software package as their requirements.
2. Purchase one of the software packages from the market (e.g. Acc Pac, Quick Books, M.Y.O.B).

There are a lot of chances of threat to their CAIS while they are using accounting software package. This has been proved by many researchers as follows.

Davis (1996) tried to discover the current status of the security issues in practice. The results of the Davis (1996) study reported that employees' accidental entry of "bad" data and the.

[1] Lecturer, Department of Commerce, Faculty of Commerce and Management, Eastern University, Sri Lanka (nrajeshm@yahoo.com)
[2] Professor of Accounting, Department of Accountancy, Faculty of Management studies and Commerce, University of Sri Jayawardenapura, Sri Lanka (kgunawardana@yahoo.com)

accidental destruction of data, as well as the introduction of computer viruses, were considered to be the three top threats in a microcomputer environment. However, unauthorized access to data and/or system by employees, accidental entry of "bad" data by employees and poor segregation of information system duties were rated as the major threats to the minicomputer environment. In respect of the mainframe computer environment, accidental entry of "bad" data by employees, natural disasters, and unauthorized access to data and/or systems by employees were perceived as the main threats, while unauthorized access to data and/or systems by both outsiders (hackers) and insiders (employees), and technology advances outpacing control practices were said to be the most important threats in a network computer environment.

In 1998, Hood and Yang studied the impact of banking information systems security on banking in China, in comparison to the UK. The survey results revealed that all respondents believe that management was aware of security but none believed that their banks had taken enough action to reduce the risks and losses. The most common reason for this was the lack of financial and human resources. Furthermore, all four banks surveyed claimed to have a security policy, but only in one was the policy formally stated. Human security threats were perceived as the most important security threats in the Chinese banking sector, especially malicious attack from outsiders.

Abu-Musa (2006) carried out a survey to investigate the perceived threats of computerized accounting information systems (CAIS) in Saudi organizations. The survey results revealed that almost half of the responded Saudi organizations were suffering financial losses due to internal and external CAIS security breaches. The results also revealed that accidental and intentional entry of bad data; accidental destruction of data by employees; employees' sharing of passwords; introduction of computer viruses to CAIS; suppression and destruction of output; unauthorized document visibility; and directing prints and distributed information to people who were not entitled to receive were the most significant perceived security threats to CAIS in Saudi organizations.

From these views, it is obvious that there are higher possibilities of threats to CAIS. These types of threats are prevailing in the developed as well as the developing countries. Those are seemed in all types of organizations without size differences. Sri Lankan organizations also are not exceptional from these threats. Hence it is assumed that these threats are prevailing in Sri Lankan organizations too.

2. PROBLEM STATEMENT

In this context, it is essential to implement adequate CAIS security controls to prevent these threats. Because of that, CAIS security controls are already implemented by the listed companies in Sri Lanka. But, there is a problem whether implementation of CAIS security controls are sufficient or not to prevent these threats in the listed companies in Sri Lanka. This research is a trial to answer the following research questions:

RQ1. Are the implemented CAIS security controls in the listed companies adequate?

RQ2. Are there significant differences among listed companies regarding the adequacy of implemented CAIS security controls?

RQ3. Which types of CAIS security controls are weak in the listed companies?

3. OBJECTIVES OF THE STUDY

The main objective of this research is to examine the existence and adequacy of implemented CAIS security controls to prevent, detect and correct security breaches in the listed companies. In addition sub objectives of this research are as follows.

i. To explore and describe significant differences among the listed companies regarding the adequacy of implemented CAIS security controls.

ii. To explore weak security controls of CAIS in the listed companies.

4. SIGNIFICANCE OF THE STUDY

The results of this study help accountants, auditors, managers, and IT users to better understand and secure their CAIS in order to achieve success of their visions. As a result, the country will be benefited by eliminate losses of organizations and improved their performance. Further there are so many researches and articles available in world wide, but in Sri Lanka it is very rear to find researches on Computerized Accounting Information Systems. Therefore, this study may lead to fill the knowledge gap on this field.

5. LITERATURE REVIEW

Information Technology was developing very fast in Sri Lanka. It was proved by following researches such as Kennedy (2005) studied potential challenges and Benefits of Implementing E-Learning in Sri Lanka by reviewing the awareness and readiness of the selected higher educational institutes. Findings revealed that Educational Institutes have also been using e-mail and Internet in addition to developing web pages for transaction of students. They have planned to invest number of funds in future in the selected areas of the e- application. Kennedy (2007) also studied the Human Resource Challenges in Information and Communication Technology (ICT) Industry in Sri Lanka and the potential for an E-Business in Sri Lanka. The study revealed that a growing demand in ICT work force. Further he noted that there was strong potentiality to go for the successful E-Business with strong involvement of companies by overcoming common problems faced by any developing country at this stage of online business. Moreover Kennedy (2008) discussed the potential challenges and benefits of information technology and economic development in Sri Lanka by reviewing the awareness and readiness of the selected opportunities. He also identified the enabling factors and bottlenecks, and forecasts the future growth of ICT developments in Sri Lanka as a host in Asia. Furthermore, developing ICT, professional services, and offshoring opportunities should be a high priority for the development strategy of the country.

In this situation, threats for CAIS are high. Reviewing the literature of the security controls of CAIS is vital. Henry (1997) conducted a survey on 261 companies in Hampton Roads, Virginia, USA, to determine the nature of their accounting systems and security in use. He attempted to ascertain the degree of correspondence between the theory and actual practice. Seven basic security methods for computerized accounting information systems were discussed and presented in his survey. These methods included encryption, password access, backup of data, virus protection, and authorisation for system changes, physical system security, and periodic audits. The results of Henry's survey indicated that 80.3 percent of the companies back-up their accounting systems, 74.4 percent of the companies secure their accounting system with passwords, but only 42.7 percent utilize protection from viruses. Physical security and authorisation for changes to the system were employed by less than 40 percent of the respondents. The survey results also showed that only 15 companies used encryption for their accounting data, which was a surprising result, considering the number of companies utilizing some form of communication hardware. Almost 45 percent of the sample underwent some sort of audit of their accounting data.

Detecting and preventing unauthorized access to CAIS by internal and external parties has become an important issue. The results of Furnell and Dowland's (2000) study revealed that traditional methods of user authentication and access security control do not provide comprehensive protection and offer opportunities for compromise by various classes of abuse.

Seetharaman, Senthilvelmurugan and Periyanayagam (2004) studied anatomy of computer accounting frauds. This paper introduced fraud as asset misappropriations (85 per cent of cases), corruption and fraudulent statements. Symptoms included accounting anomalies, lack of internal control environment, lifestyle and behaviour. The most effective tools for fraud detection were internal audit review, specific investigation by management, and whistle-blowing. The correlation of fraud perpetrators' personality with the size of losses was examined.

Personality was analyzed into age, gender, position, educational background and collusion. A strong system of internal control was most effective in fraud prevention. Fraud impacted on accounting transactions in accounts receivable, receipts and disbursements, accounts payable, inventories and fixed assets, and financial reporting. The monetary impact resulting from fraud was analyzed by the type of victim and the amount of loss. Internal control and good employment practices prevent fraud and mitigate loss. This research only touched on the surface of the computer accounting fraud. They noted future research that much more to investigate and explore on this topic especially on the techniques of committing fraud in a computerized business environment.

Abu-Musa (2004) carried out a survey to investigate the existence and adequacy of implemented CAIS security controls in the Egyptian banking sector (EBS). The results of study revealed that the vast majority of Egyptian banks have adequate CAIS security controls in place. The results also revealed 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).

Gupta and Hammond (2005) reported the results of a survey of the IS security concerns of 138 small businesses. One of the significant findings of this study was that firms continue to choose technologies which might not be very effective for their environment. Small business owners might not be adept at selecting appropriate technologies. Alternatively, their choice might be limited by affordability. Another possibility related to the nature of many small business owners. They might be too preoccupied with day-to-day operations to formulate an IS security strategy. As a consequence, they might conveniently continue to use the technology initially selected. The difficulty and cost of a switch over might be perceived as prohibitive by many small business owners, forcing them to rely on old technology.

Abu-Musha (2007b) carried out an empirical survey to investigate the existence and adequacy of implemented CAIS security controls in Saudi organizations. The paper also investigated the significant differences among different Saudi organizations as well as among respondent groups regarding the above research issues. The proposed checklist classified CAIS security controls under the following main security groups: organizational security controls, hardware and physical access security controls, software and electronic access security controls, data and data integrity security controls, off-line programs and data security controls, utilities security controls, bypassing of normal access security controls, user programming security controls, division of duties and output security controls. Most of the security controls were selected and incorporated in the questionnaire to be empirically tested in the listed companies.

Liyanagunawardena and Samarasinghe (2008) carried out research on acceptable use policy and misuse of work computers: case from Sri Lankan software development industry. The paper pointed out that organizations introduce acceptable use policies to deter employee computer misuse. Despite the controlling, monitoring and other forms of interventions employed, some employees misuse the organizational computers to carry out their personal work such as sending emails, surfing internet, chatting, playing games etc. These activities not only waste productive time of employees but also bring a risk to the organization. A questionnaire was administrated to a random sample of employees selected from large and medium scale software development organizations, which measured the work computer misuse levels and the factors that influence such behavior. The presence of guidelines provided no evidence of significant effect on the level of employee computer misuse. Not having access to Internet /email away from work and organizational settings were identified to be the most significant influences of work computer misuse.

The IT Governance Institute (ITGI, 2008) and the Information Systems Audit and Control Foundation (ISACF, 2008) developed the Control Objectives for Information and Related Technology (COBIT). COBIT provides managers, auditors, and IT users with a set of generally accepted IT control objectives to assist them in maximizing the benefits derived through the use of IT and developing the appropriate IT governance and control in their organizations. The first edition of COBIT was published in 1996. COBIT incorporates generally applicable and accepted international standards for good practice of IT management and control. Many of the COBIT security controls were selected and incorporated in the questionnaire to be empirically tested in the listed companies.

ISO 17799 also introduces a comprehensive set of controls comprising best practices in information security. It is a recognized generic international information security standard. ISO 17799 was originally published in the early 1990s as the "DTI Code of Practice" by the Department of Trade & Industry in the UK. ISO/IEC 17799 was most recently revised in June 2005 and was renamed to ISO/IEC 27002 in July 2007. The ISO 17799/ ISO 27002 standard is comprised of ten main sections: security policy, system access control, asset classification and control, personnel security, physical and environmental security, communications and operations management, access control, system development and maintenance, business continuity management, and Compliance. Many of the security controls were also selected and incorporated in the questionnaire to be empirically investigated in the listed companies.

6 HYPOTHESES

The current research is an attempt to investigate the following research hypotheses:

$H1_A$. The implemented CAIS security controls in the listed companies are adequate.

$H2_A$. There are significant differences among listed the companies regarding the adequacy of implemented CAIS security controls.

7. RESEARCH METHODOLOGY

7.1 Research design: Nature of the study was descriptive and hypothesis testing. Type of investigation was correlation. It was carried out to identify the main characteristics of the research variables. The extent of researcher interference was minimal and study setting was non contrived (natural). Time horizon was cross sectional where data collection was done over a period of several weeks. Unit of analysis was organizations.

7.2 Survey method: In this study, an empirical survey – using a self-administered questionnaire – was conducted to investigate and evaluate the existence and adequacy of implemented CAIS security controls in the selected listed companies. Most of the statements of questionnaire were adopted from Abu-Musa (2004, 2007a, 2007b) and other statements were taken from the related research papers and information security controls standards. The questionnaire used 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.

Questionnaire was pretested with academics, accountants and IT specialists. After considering the comments and suggestions of pre-test results, the revised questionnaire was piloted on a selected bank and insurance staff. Appropriate comments and suggestions were considered in developing and revising the final suggested questionnaire.

The questionnaire was classified CAIS security controls under the following main security groups: security policy, administrative security controls, hardware and physical access security controls, software and electronic access security controls, data security controls, off-line programs and data security controls, utilities security controls, bypassing of normal access security controls, separation of duties, output security controls and security controls of correct processing in applications (SCCPA).

7.3 Population and sampling: The Colombo Stock Exchange (CSE) had 236 listed companies representing 20 business sectors.

50% of population was selected as a sample. Proportionate Stratified Random Sampling method was used to select the sample companies from the CSE of population (Sekaran, 2007, p. 422). 118 questionnaires were sent by e-mail to companies but respondent rate was zero. Then questionnaires were posted to Accountants of 118 companies with self addressed stamped envelop to enable them to return the filled questionnaire. It was possible to collect less than 20 questionnaires. Hereafter follow up was done through the phone to respective Accountants. Some of them accepted to return the questionnaires at the same time some Accountants were unable to get it therefore they requested to send the questionnaires to their personnel e-mail address then questionnaires were e-mailed to them. In addition, some companies were personally visited and collected data by the researcher.

Three incomplete questionnaires were judged unusable and excluded from the data analysis. Four questionnaires were received on 29th December 2008 after completing the analysis therefore, those were not included in the study. After excluding the incomplete late and invalid responses, the research ended with 41 valid and usable questionnaires, representing a 35% response rate and 18% of the population. This response rate is considered as a high response rate in this kind of empirical survey.

7.4 Methods of data analysis: The data was analyzed using the statistical package for social sciences (SPSS) version 16. 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. Data were collected through 5 point likert scale, where 3 was determined as adequacy level.

Adequacy of CAIS Security Control = $\mu \geq 3$
Where μ is the mean of security controls.

Overall security controls was obtained by aggregating 11 types of security controls. Statistical format of above hypothesis (1) as follows,
$H1_0$. $\mu \leq 2.99$
$H1_A$. $\mu > 2.99$
Hypothesis involves the phrase "greater than", this must be a one tailed test (right tailed test). Determine whether reject the null hypothesis or not. The decision rule is: if the one-tailed critical t value is less than the observed t, then H_0 can be rejected.

One way ANOVA was used to test the significant differences among the listed companies regarding the adequacy of implemented CAIS security controls.
Make decision about null hypothesis based on

- Probability of F-statistic $\leq$ 0.05 a reject null hypothesis
- Probability of F-statistic > 0.05 a fail to reject null hypothesis

Draw conclusion about research hypothesis based on decision about null hypothesis

- Reject null hypothesis a support research hypothesis
- Fail to reject null hypothesis a do not support research hypothesis (SW318 Social Work Statistics, n.d).

8. THE RESEARCH RESULTS

The external reliability of the instrument used to collect data was examined by Test – Retest method. This test was carried out by using 10 companies from different sectors with three weeks time interval. The coefficient of the Test – Retest of the instrument indicates a high external reliability 0.993 (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 0.982 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.

	Population	Sample Size	Collected No.	Percent
Bank, Finance and Insurance	33	17	16	39.0%
Beverage Food and Tobacco	18	9	3	7.3%
Construction and Engineering	3	2	0	0.0%
Diversified holdings	11	5	2	4.9%

Figure 1 Research Sample

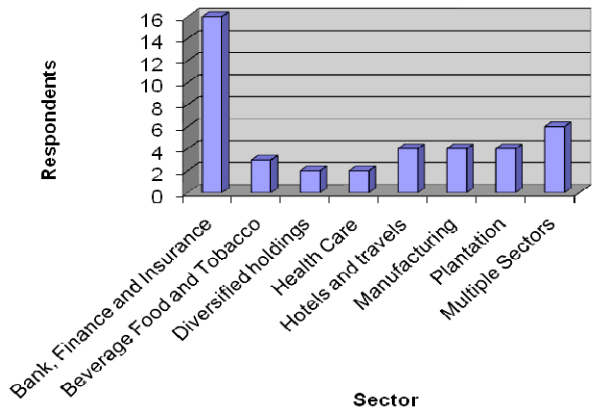

Figure 2 Research Sample

Only one questionnaire was received from the following sectors Footwear, Investment Trust, Power and Energy, Services, Stores Supplies and Trading in the current survey. For the analysis purposes, those are grouped together and named as Multiple sectors which are shown in the Figure 2.

Table 1 Security Policy

The findings of the existence and adequacy of implemented CAIS security controls and the significant differences among listed companies will be presented and discussed in the following sections.

8.1 Security Policy

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 1 the implemented Security Policies are found to be above adequate level and approaching higher security level regarding all aspects of security policies in the listed companies. Information security policy document is good or higher level in the majority of listed companies that can be assured based on mean, median, mode.

Security Policy	Mean	Std. dev.	Median	Mode
1. Information security policy document	3.85	0.727	4	4
2. Review of information security policies	3.66	0.762	4	3
3. Coordination with other security policies	3.54	0.745	3	3

Table 2 One-Sample Statistics

	N	Mean	Std. Deviation	Std. Error Mean
Security Policy	41	3.6829	0.68293	0.10666
Administrative Security Control	41	3.2724	0.68694	0.10728
Hardware and physical access security controls	41	3.8333	0.67726	0.10577
Software and electronic access security controls	41	3.9961	0.71774	0.11209
Data security controls	41	3.8073	0.68898	0.10760
Off-line programs and data security controls	41	3.5427	0.73930	0.11546
Utilities security controls	41	3.3984	1.03339	0.16139
Bypassing of normal access security controls	41	3.4472	0.99892	0.15600
Separation of duties	41	3.9187	0.66575	0.10397
Output security controls	41	3.7073	0.80701	0.12603
SCCPA	41	3.9512	0.74372	0.11615
Overall Security Controls	41	3.6870	0.60991	0.09525

The critical t(d.f 40, α=0.05) is 1.6839 and the observed t is 6.497, H1(i)0 is rejected and H1(i)A is accepted at 5% significant level. That is, there is sufficient evidence to conclude that the mean number of Security Policy is larger than 2.99 and the implemented Security Policies of CAIS in the listed companies are adequate (Table 2 and 3).

Table 4 reveals the significance is 0.550, which is greater than 0.05. So, the variances are approximately equal for Security Policy. ANOVA table shows there are no significant differences among the listed companies regarding the existence and the implementation of the security policy of CAIS at significance level 0.05.

8.2 Administrative Security Controls

As indicated by mean values in the Table 6 Administrative Security Controls are found to be above adequate level in the listed companies except Mandatory vacations used to reduce the fraud resulting from increased chance of exposure. But only positive management attitude toward the security of CAIS is higher level and it falls between categories of good and perfect level.
More than 50% of companies reported that rotation of duties helped to identify the errors and irregularities are good or higher level that was assured by median and mode.

On the other hand, mean number of mandatory vacations used to reduce the fraud resulting from increased chance of exposure is 2.66 with standard deviation 1.257. Thus many of listed companies fall between categories of not at all and poor level. Moreover, most of responded companies - personnel policies include background checks to reduce the hiring dishonest employees, there is documentation showing that users have been properly trained and the employees who have access to sensitive data have been bonded (agreement) are between poor and adequate level.

The critical t is 1.6839 and the observed t is 2.632, there is 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 are adequate. The ANOVA Table 5 reveals there are significant differences among the listed companies regarding the existence and the implementation of the Administrative Security Controls of CAIS at significance level 0.05. The mean of Beverage, Food and Tobacco sector and the Plantation sector are significantly different than other sectors for Administrative Security Controls.

Table 3 One-Sample t test

	Test Value = 2.99					
	t	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
Security Policy	6.497	40	0.000	0.6929	0.4774	0.9085
Administrative Security Control	2.632	40	0.012	0.2824	0.0655	0.4992
Hardware and physical access security controls	7.973	40	0.000	0.8433	0.6296	1.0571
Software and electronic access security controls	8.976	40	0.000	1.0061	0.7796	1.2327
Data security controls	7.596	40	0.000	0.8173	0.5998	1.0348
Off-line programs and data security controls	4.787	40	0.000	0.5527	0.3193	0.7860
Utilities security controls	2.530	40	0.015	0.4084	0.0822	0.7346
Bypassing of normal access security controls	2.930	40	0.006	0.4572	0.1419	0.7725
Separation of duties	8.932	40	0.000	0.9287	0.7186	1.1388
Output security controls	5.691	40	0.000	0.7173	0.4626	0.9720
SCCPA	8.276	40	0.000	0.9612	0.7265	1.1960
Overall Security Controls	7.318	40	0.000	0.6970	0.5045	0.8896

Table 4 Test of Homogeneity of Variances

	Levene Statistic	df1	df2	Sig.
Security Policy	0.857	7	33	0.550
Administrative Security Control	0.895	7	33	0.522
Hardware and physical access security controls	1.466	7	33	0.214
Software and electronic access security controls	1.390	7	33	0.243
Data security controls	1.608	7	33	0.168
Off-line programs and data security controls	2.071	7	33	0.075
Utilities security controls	1.583	7	33	0.175
Bypassing of normal access security controls	0.917	7	33	0.506
Separation of duties	1.073	7	33	0.403
Output security controls	1.815	7	33	0.117
SCCPA	2.170	7	33	0.063
Overall Security Controls	1.536	7	33	0.190

8.3 Hardware and Physical Access Security Controls

The results reveal that mean value and standard deviation of implemented un-interruptible power supply units to supply power during power outages are 4.32 and 0.82 respectively. It indicated that majority of responded companies use generators during the power failure. Further, 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), communications lines (e.g. cables should be sealed in ducts outside the hardware area to prevent tapping or reading by service equipment) is around 4 and fall under the higher and perfect level (Table 7).

Table 5 ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
Security Policy	Between Groups	5.461	7	0.780	1.951	0.093
	Within Groups	13.194	33	0.400		
Administrative Security Control	Between Groups	6.952	7	0.993	2.749	0.023
	Within Groups	11.924	33	0.361		
Hardware and physical access security controls	Between Groups	5.081	7	0.726	1.806	0.119
	Within Groups	13.266	33	0.402		
Software and electronic access security controls	Between Groups	6.514	7	0.931	2.179	0.062
	Within Groups	14.092	33	0.427		
Data security controls	Between Groups	6.253	7	0.893	2.315	0.049
	Within Groups	12.734	33	0.386		
Off-line programs and data security controls	Between Groups	9.382	7	1.340	3.544	0.006
	Within Groups	12.480	33	0.378		
Utilities security controls	Between Groups	20.799	7	2.971	4.474	0.001
	Within Groups	21.917	33	0.664		
Bypassing of normal access security controls	Between Groups	17.024	7	2.432	3.506	0.006
	Within Groups	22.889	33	0.694		
Separation of duties	Between Groups	4.979	7	0.711	1.841	0.112
	Within Groups	12.750	33	0.386		
Output security controls	Between Groups	9.491	7	1.356	2.702	0.025
	Within Groups	16.559	33	0.502		
SCCPA	Between Groups	5.724	7	0.818	1.645	0.157
	Within Groups	16.400	33	0.497		
Overall Security Controls	Between Groups	5.911	7	0.844	3.107	0.012
	Within Groups	8.969	33	0.272		

Table 6 Administrative Security Controls

Administrative Security Controls	Mean	Std. dev.	Median	Mode
1. Management attitude toward the security of CAIS is positive	4.32	0.650	4	4
2. Rotation of duties helped to identify the errors and irregularities	3.41	0.741	4	4
3. Mandatory vacations used to reduce the fraud resulting from increased chance of exposure	2.66	1.257	3	3
4. Personnel policies include background checks to reduce the hiring dishonest employees	3.12	0.927	3	3
5. There is documentation showing that users have been properly trained	3.12	0.980	3	3
6. The employees who have access to sensitive data have been bonded (agreement)	3	1.225	3	3

The median values of the Table 7 also indicates that more than 50% of respondents are higher security control in respect of implemented installing computers only in areas that are locked and kept under close watch when not in use, 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 should be independent of programming, system software, and accounting control functions while rest of them fall into categories of adequate and good level.

On contrast, mean value of installing alarms and video camera in areas with high

concentration of computer equipment is 2.88 and standard deviation is also high (1.308). Therefore, it is noted that several responded companies are poor in relating to implemented installing alarms and video camera in high concentration of computer equipment areas.

The critical t is 1.6839 and the calculated t is 7.973, there is sufficient evidence to conclude that the mean number of Hardware and Physical Access Security Controls is larger than 2.99 and the implemented Hardware and Physical Access Security Controls of CAIS in the listed companies are adequate (Table 2 and 3). There are 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 0.05 (Table 4 and 5).

8.4 Software and Electronic Access Security Controls

From Table 8, Majority of the companies' respondents confirmed the installation of virus production software in their computerized accounting systems is perfect which is proved by mean median and mode value. Mean and median values of password procedures are more than 4; high respondents confirmed that strong password systems are used to identify individuals to the system as authorized users. Higher security procedures are implemented to ensure that the passwords are periodically changed, kept secret, and could not easily be guessed. Passwords are typically immediately cancelled for terminated or transferred company employees. Moreover, mean value indicated that there is higher security control

Table 7 Hardware and Physical Access Security Controls

Hardware and Physical Access Security Controls	Mean	Std. dev.	Median	Mode
1. Theft and hazard insurance covering computers' hardware	3.98	1.037	4	4
2. Limiting computer access to employees with a defined need	3.93	0.755	4	4
3. Installing computers only in areas that are locked and kept under close watch when not in use	3.46	1.051	4	4
4. Installing alarms and video camera in areas with high concentration of computer equipment	2.88	1.308	3	2
5. Un-interruptible power supply units to supply power during power outages	4.32	0.820	4	4
6. Protection of computers from water, smoking and dust	4	0.742	4	4
7. There are controls to restrict physical access to the following:				
A. Terminals	3.95	0.973	4	4
B. Computer room	4.22	0.881	4	5
C. Hardware outside the computer room (e.g. network switch-gear, modems)	4.07	0.932	4	4
D. Communications lines (e.g. cables should be sealed in ducts outside the hardware area to prevent tapping or reading by service equipment)	3.95	0.999	4	5
8. Controls over the generating and revoking the means of permitting physical access (e.g. key, security badge, combination number, switch card)	3.66	1.109	4	4
9. The person responsible for controlling physical access should be independent of programming, system software, and accounting control functions	3.59	1.024	4	4

Table 8 Software and Electronic Access Security Controls

Software and Electronic Access Security Controls	Mean	Std. dev.	Median	Mode
1. Virus protection software should be installed	4.44	0.743	5	5
2. Sensitive data transmitted should be encrypted	4	1.025	4	4
3. The present insurance should cover software	3.78	1.314	4	4
4. Software backups, like originals, should have write-protect tabs in place	3.98	0.821	4	4
5. Originals placed in an off –site storage (e.g. a safe-deposit box or the home of the owner or chief executive officer)	3.76	1.090	4	4
6. Steps should be taken to avoid unauthorized copying of licensed software	3.95	1.024	4	5
7. Steps should be taken to avoid the use of illegal software	4.02	0.880	4	5
8. Are there controls over:				
A. Assigning access rights to appropriate individual in the organization	4.07	0.932	4	5
B. Allocating and withdrawing special facilities from users (e.g. ability to use certain utilities, higher levels of clearance in a hierarchy)	4.22	0.759	4	5
C. Protecting the security tables stored on the system, which are used by the system to verify authenticity (e.g. password control files, communication control tables can be one-way encrypted)	4.12	0.927	4	5
9. Are there procedures to ensure that the passwords (or other codes) are:				
A. Periodically changed	4.37	0.799	5	5
B. Kept secret (e.g. not written down or displayed on screen)	4.24	0.860	4	5
C. Not easily guessed, and	4.20	0.749	4	4
D. Cancelled for terminated or transferred employees	4.29	0.844	4	5
10. Procedures should be implemented to ensure the ability to use the following access control functions are itself restricted to appropriate staff with no other incompatible duties:				
A. Granting or changing systems identities	3.85	0.792	4	3
B. Granting or changing the ability to use special facilities	3.76	0.888	4	3
C. Changing passwords or other identification codes	3.90	0.831	4	3
11. Firewall security control	3.88	1.005	4	4
12. Security controls of mobile computing and teleworking	3.10	1.375	3	4

over assigning access rights to appropriate individuals in the responded companies. The most of respondents also confirmed the allocating and withdrawing special facilities from users (for example, ability to use certain utilities, hierarchical levels of clearance) and protection of security tables stored on the system to verify authenticity (password control files, or communication control tables which can be one-way encrypted) are between high and perfect level.

Statistical results of Table 8 shows that mean value of software relating to backups, off –

Table 9 Data Security Controls

Data Security Controls	Mean	Std. dev.	Median	Mode
1. Security controls implemented over manual handling of input and output data among the organization's departments	3.98	0.880	4	4
2. Data backups should be routinely prepared	4.24	0.699	4	4
3. A copy of backups should be placed in an off-site storage	4.10	0.860	4	5
4. Backups of sensitive data that are stored off-site should be encrypted to reduce the chance of unauthorized exposure	3.68	1.105	4	4
5. A hard copy should be routinely printed for particularly critical data	3.90	0.970	4	5
6. The FORMAT command should be left off the hard disk	3.37	1.280	4	4
7. Data encryption should be considered for sensitive data (e.g. payroll)	3.61	1.022	4	3
8. Reformatting of the disk or overwriting of the file should be required for extraction of sensitive data	3.66	0.965	4	4
9. A documented emergency plan should state				
A. The main steps that should be taken when systems fail	3.76	0.860	4	3
B. Who is responsible for completion of the steps	3.78	0.822	4	3

site storage, avoid unauthorized copying of licensed software and avoid the use of illegal software are almost 4 and fall into categories of higher level. Sensitive data transmitted should be encrypted is fall into interval of adequate and higher level because mean value and standard deviation are 4 and more than one respectively.

Access control functions are themselves restricted to appropriate staff with no other incompatible duties and firewall security control also above adequate level. Security controls of mobile computing and teleworking are falling between poor and adequate level but in the banking sector it is above the adequate level.

The critical t is 1.6839 and the calculated t is 8.976, Table 2 and 3 reveal there is sufficient evidence to conclude that the mean number of Software and Electronic Access Security Controls is larger than 2.99 and the implemented Software and Electronic Access Security Controls of CAIS in the listed companies are adequate. There are no significant differences among the listed companies regarding the existence and the implementation of the Software and Electronic Access Security Controls of CAIS at alpha = 0.05 (Table 4 and 5).

8.5 Data Security Controls

The results reveal that in the Table 9, mean value of data backup routinely prepared and off-site storage of backup copy are more than 4 and fall into higher or good level security controls in the listed companies. Further, the security controls over the manual handling of input and output data and a hard copy routinely printed for particularly critical data are also good level in the responded companies. Mean and median values indicate the existence of documented emergency plans, which stated the main steps that should be taken when the systems failed, as well as the individuals who were responsible for completion of these steps are fall between categories of adequate and good level.

More than 50% of companies reported that encryption of backup and sensitive data are higher level whereas many companies falls into categories of poor and adequate level because standard deviation is more than one.

Table 10 Off-Line Programs and Data Security Controls

Off-Line Programs and Data Security Controls	Mean	Std. dev.	Median	Mode
1. Where programs and data, including back-up copies, are physically controlled:				
A. Records should be kept to identify programs/data uniquely (e.g. external labels)	3.59	0.836	4	3
B. Security controls should be implemented over issuing and returning of programs/data files	3.61	0.891	4	4
C. Storage methods should prevent the unauthorized removal of programs/data (e.g. diskettes/ flash drive)	3.61	0.891	4	4
2. The librarian function should be performed by a person independent of computer operation and programming responsibilities	3.67	1.135	3	3

On the other hand, mean and standard deviation of the format command should be left off the hard disk indicated that many companies fall into poor and adequate level while financial sector is above higher level.

The critical t is 1.6839 and the observed t is 7.596, there is sufficient evidence to conclude that the mean number of Data Security Controls is larger than 2.99 and the implemented Data Security Controls of CAIS in the listed companies are adequate(Table 2 and 3). There are significant differences among the listed companies regarding the existence and the implementation of the Data Security Controls of CAIS (α =0.05). The mean of Bank, Finance and Insurance sector and the Plantation sector are significantly different than other sectors for Data Security Controls (Table 4 and 5).

8.6 Off-Line Programs and Data Security Controls

Table 10 explains Off-Line Programs and Data Security Controls means programs and data, including back-up copies, are physically controlled such as records should be kept to identify programs/data uniquely (e.g. external labels), Security controls should be implemented over issuing and returning of programs/data files and Storage methods should prevent the unauthorized removal of programs/data (e.g. diskettes/ flash drive). Mean values of above security controls is more than 3.5 and those security controls move towards good level.

On the other hand, more than 50% of respondents noted that librarian functions in their companies were not adequately performed by independent person of computer operation and programming responsibilities. Furthermore, this security control of listed companies fall between poor and good level

The critical t is 1.6839 and the calculated t is 4.787, there is sufficient evidence to conclude that the mean number of Off-Line Programs and Data Security Controls is larger than 2.99 and the implemented Off-Line Programs and Data Security Controls of CAIS in the listed companies are adequate (Table 2 and 3). There are significant differences among the listed companies regarding the existence and the implementation of the Off-Line Programs and Data Security Controls of CAIS at significance level 0.05 (Table 4 and 5). The mean of Bank, Finance and Insurance sector and the Plantation sector are significantly different than other sectors for Off-Line Programs and Data Security Controls.

8.7 Utilities Security Controls

The statistical Table 11 shows that all aspects of implemented utility program are above the adequate level but standard deviation of utility program is above one. It means that a lot of companies fall between the poor and good level. More than 50% of the companies mentioned that implemented procedures to identify such program and implemented security controls to log and report the use, or attempted use, of such programs are good level. 50% of respondents reported the ability to use such programs should be adequately

Table 11 Utilities Security Controls

Utilities Security Controls	Mean	Std. dev.	Median	Mode
1. Utilities or other special programs could be used to change application programs/data by bypassing normal software access restrictions:				
A. Procedures should be implemented to identify all programs with this special status	3.37	1.043	4	4
B. The ability to use such programs should be restricted to appropriate, authorized personnel in the organizations	3.44	1.097	3	3
C. Security controls to log and report the use, or attempted use, of such programs should be implemented. A review of such reports should be performed by a responsible official to determine and investigate unauthorized access	3.39	1.115	4	4

Table 12 Bypassing of Normal Access Security Controls

Bypassing of Normal Access Security Controls	Mean	Std. dev.	Median	Mode
1. Where it is necessary to bypass normal security controls (e.g. emergencies or maintenance of program libraries by outside software support, such as vendor, through dial up):				
A. Is there appropriate authorization before or after the event	3.56	1.074	4	4
B. Are there controls to:				
i. Ensure that security is subsequently reinstated	3.41	1.048	4	4
ii. Prevent or report and investigate unauthorized changes to data	3.37	1.043	4	4

restricted to appropriate, authorized personnel in the organizations.

The critical t is 1.6839 and the observed t is 2.530, Table 2 and 3 reveal there is sufficient evidence to conclude that the mean number of Utilities Security Controls is larger than 2.99 and the implemented Utilities Security Controls of CAIS in the listed companies are adequate. There are significant differences among the listed companies regarding the existence and the implementation of the Utilities Security Controls of CAIS at significance level 0.05 (Table 4 and 5). The mean value of Bank, Finance and Insurance sector is significantly different from the Plantation and Multiple Sectors for Utilities Security Controls.

8.8 Bypassing of Normal Access Security Controls

Bypassing is necessary in the case of emergencies or maintenance of program libraries by outside software support, such as vendor, through dial up. In this scenario it is very important to do such actions under the security controls. The Table 12 shows that 50% of responded companies are higher security level regarding bypass at the same time rest of them fall into poor and adequate level.

The critical t is 1.6839 and the observed t is 2.930, there is sufficient evidence to conclude that the mean number of Bypassing of Normal Access Security Controls is larger than 2.99 and the implemented Bypassing of Normal Access Security Controls of CAIS in the listed companies are adequate (Table 2 and 3). There are significant differences among the listed companies regarding the existence and the implementation of the Bypassing of Normal Access Security Controls of CAIS at significance level 0.05 (Table 4 and 5). The mean of Bank, Finance and Insurance sector and the Plantation sector are significantly

Table 13 Separation of Duties

Separation of Duties	Mean	Std. dev.	Median	Mode
1. Level of segregation of accounting duties (i.e., authorization, record keeping, and custody)	4.02	0.758	4	4
2. Level of controls to prevent:				
A. Computer operators, schedulers, data input staff, and other operations personnel from gaining access to program documentation and development libraries	3.95	0.705	4	4
B. Development personnel from gaining access to the computer operations area	3.78	0.822	4	4

Table 14 Output Security Controls

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	4.17	0.667	4	4
2. Printing of sensitive data outside the data centre or central computer room should be under security controls	4	0.775	4	4
3. Sensitive computer output should be secured in a locked cabinet	3.80	0.813	4	4
4. Hard copy output should be automatically date/time stamped	3.63	1.135	4	4
5. Security controls should be implemented over printed copies of data/information	3.76	0.860	4	3
6. Printing and distribution of data and information done should be under proper security controls, and only by authorized persons in the organization	3.98	0.908	4	4
7. Shredding (cutting) machines should be available and used for disposal of confidential data	3.24	1.220	3	3
8. Shredding of sensitive documents should be restricted to security cleared personnel	3.07	1.367	3	3

different than other sectors for Bypassing of Normal Access Security Controls.

8.9 Separation of Duties

From Table 13, mean value of level of segregation of accounting duties is above 4 and standard deviation is around 0.8 which indicated that separation of accounting duties is a higher level in the listed companies. Computer operators, schedulers, data input staff, and other operations personnel from gaining access to program documentation and development libraries are also almost higher level. Moreover, restriction of development personnel from gaining access to the computer operations area falls between categories of adequate and good level.

The critical t is 1.6839 and the calculated t is 8.932, Table 2 and 3 indicate that there is sufficient evidence to conclude that the mean number of Separation of Duties is larger than 2.99 and the implemented Separation of Duties of CAIS in the listed companies are adequate. There are no significant differences among the listed companies regarding the existence and the implementation of the Separation of Duties of CAIS at 5% significance level (Table 4 and 5).

8.10 Output Security Controls

Table 14 shows that mean value of visual access of sensitive data, printing of sensitive data outside the data centre or central computer room and sensitive computer output secured in a locked cabinet almost 4 and

Table 15 Security Controls of Correct Processing in Applications

Security Controls of Correct Processing in Applications	Mean	Std. dev.	Median	Mode
1. Input data validation - Use of both automatic and manual methods of data verification and cross-checking, as appropriate	3.98	0.758	4	4
2. Control of internal processing -Validation checks should be incorporated into applications to detect the corruption of information through processing errors or deliberate acts.	3.98	0.758	4	4
3. Output data validation - Random output/input comparisons should be regularly done to verify correct processing.	3.90	0.860	4	3

above and it indicates a higher level of output security controls. Mean and standard deviation of hard copy output automatically date and time stamped are 3.63 and 1.135 respectively and this security control fall between poor and higher level.

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 poor and adequate level. It is proved by values of mean and standard deviation.

The critical t is 1.6839 and the observed t is 5.691, there is 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 are adequate (Table 2 and 3). There are significant differences among the listed companies regarding the existence and the implementation of the Output Security Controls of CAIS at $\alpha = 0.05$ (Table 4 and 5). The mean of Bank, Finance and Insurance sector and the Plantation sector are significantly different than other sectors for Output Security Controls.

8.11 Security Controls of Correct Processing in Applications (SCCPA)

The Table 15 reveals that mean and standard value of input data validation, control of internal processing and output data validation are approximately 4 and 0.8 respectively. It indicated that SCCPA fall into adequate and good level. Further, more than 50% of responded companies mentioned that these controls more than higher level.

The critical t is 1.6839 and the observed t is 8.276, there is sufficient evidence to conclude that the mean number of SCCPA is larger than 2.99 and the implemented SCCPA of CAIS in the listed companies are adequate (Table 2 and 3). Table 4 and 5 reveal there are no significant differences among the listed companies regarding the existence and the implementation of the SCCPA of CAIS at significance level 0.05.

9. CONCLUSION

In this study an empirical survey was carried out to investigate the existence and adequacy of implemented CAIS security controls in the listed companies in Sri Lanka. This study also investigated the significant differences among the listed companies regarding the above research issue. In addition this study found weak security controls of CAIS. Results of one sample t test revealed all the implemented CAIS security controls were adequate level. 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. 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, off-line programs and data security controls, utilities security controls, bypassing of normal

access security controls and output security controls were 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.

10. RECOMMENDATIONS

Recommendations are given in following areas to eliminate weaknesses and strengthen the implemented CAIS security controls for short and long terms.

10.1 Short term

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

10.1.2 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.

10.1.3 Hardware and physical access security controls: Companies are recommended to install video camera 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.

10.1.4 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.

10.1.5 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.

10.1.6 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.

10.1.7 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.

10.1.8 Bypassing of normal access security controls: Strict security should be implemented regarding the bypassing of normal access controls to prevent, investigate and report any unauthorized changes to companies' data files. Higher security controls should be in place to ensure that security is subsequently reinstated whenever bypassing of normal security controls has occurred in emergency cases.

10.1.9 Separation of duties: Already separation of duties is higher level in the listed companies but it should uplift to perfect level. Stronger procedure should be put in place to prevent computer operators, schedulers, data input staff, and other operations personnel from gaining access to program documentation and development libraries.

Increase level of control to prevent development personnel from gaining access to the computer operations area

10.1.10 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.Almost output security controls were higher level but they should take more actions on what was mentioned in the questionnaire under the output security controls to reach perfect level.

10.1.11 Security controls of correct processing in applications: Statistics of SCCPA reveals that they have already paid adequate controlling methods to eliminate errors. But, still it is in the adequate and higher level. Therefore, they must pay more attention for input data validation, control of internal processing and output data validation to get in touch with perfect level.

10.2 Long term

10.2.1 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.

10.2.2 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.

10.2.3 Hardware and physical access security controls: *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.

11. FUTURE RESEARCH

The intention of the current research has been to investigate the security controls of CAIS in the listed companies. One weakness of this study is that it has only dealt with the listed companies at Colombo Stock Exchange. However, more research is needed to obtain evidence from other companies and Government sectors in Sri Lanka. Comparative studies could be carried out to investigate the significant differences between developing and developed countries regarding the adequacy and effectiveness of implemented CAIS security controls.

12. IMPLICATIONS OF THE STUDY

Most of the CAIS security controls were studied by previous researchers as a little by little (section by section) but this study was done comprehensively (holistic). Therefore, this questionnaire can be used by any organization for self evaluating its CAIS security controls. Further Findings and recommendations of this study help accountants, auditors, managers, and IT users to better understand and secure their CAIS in order to achieve success of their visions.

REFERENCES

Abu-Musa, A. A. (2004). "Investigating the security controls of CAIS in an emerging economy: an empirical study on Egyptian banking industry", *The Journal of Managerial Auditing*, Emerald Group Publishing Limited, Vol. 19 No. 2, pp. 272-302. [Online], Available: http://emeraldinsight.com/Insight/viewPDF.jsp?Filename=html/Output/Published/EmeraldFullTextArticle/Pdf/0510190207.pdf, [07/09/2008].

Abu-Musa, A. A. (2006). "Exploring perceived threats of CAIS in developing countries: the case of Saudi Arabia", *Managerial Auditing Journal*, Emerald Group Publishing Limited, Vol. 21 No. 4. pp. 387-407 [Online], Available: http://www.emeraldinsight.com/0268-6902.htm, [29/01/2008].

Abu-Musa, A. A. (2007a). "Evaluating the security controls of CAIS in developing countries: An examination of current research", *Information Management and Computer Securit*y, Emerald Group Publishing Limited, Vol. 15 No. 1, 2007 pp. 46-63 [Online], Available:

http://emeraldinsight.com/Insight/viewPDF.jsp?Filename=html/Output/Published/EmeraldFullTextArticle/Pdf/0460150104.pdf, [07/09/2008].

Abu-Musa, A. A. (2007b). "Evaluating the security controls of CAIS in developing countries: an empirical investigation", *Information Management and Computer Security*, Emerald Group Publishing Limited, Vol. 15 No.2, pp.128-148, [Online], Available: http://www.emeraldinsight.com/0968-5227.htm, [05/03/2008].

Boritz, J. E. (1999). Computer Control and Audit Guide, [Online] available: http://arts.unwareloo.co/ACCA/ccag

Colombo Stock Exchange, (2008). *Industry sector,* [Online], Available: http://www.cse.lk/welcome.htm, [29/03/2008], [25/04/2008].

Courtney, H. M., Cheryl, L. P. and Terryann, G. (1998). "Guide to accounting software: the pluses and minuses of nine leading mid-price-range products", Journal of Accountancy, Vol. 185 No. 3, pp. 44-61.

Davis, C. E. (1996). 'Perceived security threats to today's accounting information systems: a survey of CISAs', *IS Audit & Control Journal*, Vol. 3, pp. 38-41.

Dhillon, G. (1999). "Managing and controlling computer misuse", *Information Management & Computer Security*, Vol. 7 No. 4, pp. 171-5.

Dhillon, G. and Backhouse, J. (2000). "Information systems security management in the new millennium", *Association for Computing Machinery*, *Communication of the ACM,* Vol. 43 No. 7, pp. 125-9.

Furnell, S. M. and Dowland, P. S. (2000). "A conceptual architecture for real-time intrusion monitoring", *Information Management & Computer Security*, Vol. 8 No. 2, pp. 65-75.

Gupta, A. and Hammond, R. (2005). "Information systems security issues and decisions for small businesses: An empirical examination" *Information Management & Computer Security,* Vol. 13 No. 4, pp. 297-310 [Online], Available: http://www.emeraldinsight.com/Insight/viewPDF.jsp?Filename=html/Output/Published/EmeraldFullTextArticle/Pdf/0460130404.pdf, [13/08/2008].

Hermanson, D. R., Hill, M. C. and Ivancevich, D. M. (2000). "Information technology-related activities of internal auditors", *Journal of Information Systems*, Supplement, Vol. 14 No. 1, pp. 39-53.

Hester, E. D. and Andrew, C. G. (1998). "Industry corner: the information security marketplace", *Business Economics*, Vol. 33 No. 2, pp. 52-6.

Hood, K. L. and Yang, J. (1998). "Impact of banking information systems security on banking in China: the case of large state-owned banks in Shenzhen economic special zone – an introduction", *Journal of Global Information Management*, Vol. 6 No. 3, pp. 5-15.

Hunton, J., Wright, A. and Wright, S. (2005). "Are financial auditors overconfident in their ability to assess risks associated with enterprise resource planning systems?", *Journal of Accounting Information Systems*, Vol. 18 No. 2, pp. 7-28.

Information Technology – Code of practice for Information Security Management ISO/IEC 17799 ISO/IEC 27002 (2005). [Online], Available: http://www.17799central.com/iso17799.htm [23/08/2008] http://privacy.med.miami.edu/glossary/xd_iso_27002_index.htm [15/10/2008].

ISACF (2008). Control Objectives for Information and Related Technology (COBIT), Information Systems Audit and Control Foundation, Rolling Meadows, IL. [Online], Available: http://www.isaca.org/Template.cfm?Section=COBIT_Online&Template=/ContentManagement/ContentDisplay.cfm&ContentID=15633 [08/09/2008]

ITGI (2008). Board Briefing on IT Governance, IT Governance Institute [Online], available: www.itgi.org/ [08/09/2008]

Kankanhalli, A., Teo, H., Tan, B. and Wei, K. (2003). "An integrative study of information systems security effectiveness", *International Journal of Information Management*, Vol. 23 No. 2, p. 139.

Kennedy, D. G. (2005). "An Empirical Study of potential challenges and Benefits of Implementing E-learning in Sri Lanka", Special Issue of the International Journal of The Computer, the Internet and Management, pp.33.1-8 [Online], Available: http://www.elearning.au.edu/research/elear

ning_conference_2005/Proceeding2005%20and%20Book/PP33.pdf, [15/06/2008].

Kennedy, D. G. (2007). "Human Resource Challenges to develop eBusiness in Sri Lanka - a Case Study" Special Issue of the International Journal of the Computer, the Internet and Management, Vol.15 No. SP4, [Online], Available: http://www.ijcim.th.org/v15nSP4/P20SEARCC_HRChallengestodevelopeBusinessinSriLanka.pdf. [13/09/2008].

Kennedy, D. G. (2008). "Potential Challenges and Benefits of Information Technology and Economic Development in Sri Lanka", Information Technology and Economic Development, Japan: Information Science Reference, [Online], Available:https://igi-pub.com/reference/details.asp?ID=6921&v=tableOfContents, [27/10/2008].

Laudon, K. C. and Laudon, J. P. (2006). Management Information System – Managing the digital firm, 9th ed., New Jersey: Prentice-Hall, pp340-68

Romney, M. and Steinnbart, P. (2006). *Accounting Information Systems*, 10th ed., New Jersey: Pearson Prentice Hall.

Ryan, S.D. and Bordoloi, B. (1997). "Evaluating security threats in mainframe and client/server environments", *Information & Management*, Vol. 32 No. 3, pp. 137-42.

Seetharaman A., Senthilvelmurugan M. and Periyanayagam R. (2004). Anatomy of computer accounting frauds, Managerial Auditing Journal, Emerald Group Publishing Limited, Vol. 19 No. 8, pp. 1055-1072 [online] available: http://emeraldinsight.com/Insight/viewPDF.jsp?Filename=html/Output/Published/EmeraldFullTextArticle/Pdf/0510190807.pdf, [07/09/2008].

Sekaran, U. (2007). *RESEARCH METHODS FOR BUSINESS A Skill Building Approach*, 4th ed., New Delhi: Wiley India (P.) Ltd.

Spinellis, D., Kokolakis, S. and Gritzalis, S. (1999). "Security requirements, risks and recommendations for small enterprise and home-office environments", *Information Management & Computer Security*, Vol. 7 No. 3, pp. 121-8.

SW318 Social Work Statistics, (n.d.). One-way Analysis of Variance, [Online], Available: www.utexas.edu/courses/schwab/sw318_spring_2004/SolvingProblems/Class25_ANOVA.ppt, [17/10/2008].

Using SPSS for t-Tests (n.d.). Using SPSS for t-Tests, [Online], Available: http://academic.udayton.edu/GregElvers/psy216/SPSS/ttests.htm, [26/10/2008].

Warren, M.J. (2002). "Security practice: survey evidence from three countries", *Logistics Information Managemen*t, Vol. 15 Nos 5/6, pp. 347-51.

Wikipedia. (2008). *Separation of duties,* [Online], Available: http://en.wikipedia.org/wiki/Separation_of_duties, [06/10/2008].

Wood, F. and Sangster, A. (2007). *Business Accounting 1,* 10th ed., India: Dorling Kindersley (India) pvt. Ltd. pp. 234-258.

Wright, S. and Wright, A. (2002). "Information system assurance for enterprise resource planning systems: implementation and unique risk considerations", *Journal of Information Systems*, Vol. 16, Supplement, pp. 99-113.

Zviran, M. and Haga, W.J. (1999). "Password security: an empirical study", *Journal of Management Information Systems*, Vol. 15 No. 4, pp. 161-85.