

INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATION & MANAGEMENT

IJR
CM



A Monthly Double-Blind Peer Reviewed (Refereed/Juried) Open Access International e-Journal - Included in the International Serial Directories

Indexed & Listed at:

Ulrich's Periodicals Directory ©, ProQuest, U.S.A., EBSCO Publishing, U.S.A., Cabell's Directories of Publishing Opportunities, U.S.A.

Open J-Gate, India [link of the same is duly available at Infibnet of University Grants Commission (U.G.C.)]

Index Copernicus Publishers Panel, Poland with IC Value of 5.09 & number of libraries all around the world.

Circulated all over the world & Google has verified that scholars of more than 2255 Cities in 155 countries/territories are visiting our journal on regular basis.

Ground Floor, Building No. 1041-C-1, Devi Bhawan Bazar, JAGADHRI – 135 003, Yamunanagar, Haryana, INDIA

<http://ijrcm.org.in/>

CONTENTS

Sr. No.	TITLE & NAME OF THE AUTHOR (S)	Page No.
1.	RELATIVE POVERTY AND INEQUALITY – A STUDY OF HIMACHAL PRADESH RAMNA	1
2.	SUSTAINING EMPLOYEE ENGAGEMENT IN THE FACE OF CRISIS – A TEST OF LEADERSHIP AND INTRODUCTION OF A NEW MODEL JAYDEEP H GOSWAMI	8
3.	AN EXPLORATORY STUDY ON CONSUMERS' ENVIRONMENTAL ATTITUDE ABOUT GREEN ELECTRONIC PRODUCTS IN ANKLESHWAR DR. AMIT R. PANDYA & PRATIK M. MAVANI	13
4.	JPEG IMAGE COMPRESSION ALGORITHM CHETAN DUDHAGARA & DR. KISHOR ATKOTIYA	20
5.	DO EMPLOYEES LACK IN REQUIRED SKILLS: AN ANALYSIS ON SIGNIFICANT SKILLS REPORTED FOR EMPLOYEES IN ORGANIZED RETAIL SECTOR & EXISTING GAP WITHIN DR. MANOJ VERGHESE & SUSHIL PUNWATKAR	26
6.	AN ANALYSIS OF INCOME STATEMENT OF A SERVICE SECTOR UNDERTAKING – A CASE STUDY OF INDUSTRIAL FINANCE CORPORATION OF INDIA LTD DR. SANTOSH GUPTA, SOMA NAG & AMIT NAG	30
7.	SIZE, AGE AND GROWTH IN INDIAN SELECTED PHARMACEUTICAL COMPANIES N. CHANDRIKA & DR. G. V. CHALAM	37
8.	VENTURE CAPITAL FIRMS ASSESSMENT CRITERIA'S WHILE FINANCING FOR NEW ENTERPRISES IN KARNATAKA SRINIVAS K T & DR. N NAGARAJA	41
9.	INVESTIGATING STOCK MARKET EFFICIENCY IN INDIA SAHANA PRASAD	45
10.	INNOVATING ICT FOR GENDER SENSITIVE DEVELOPMENT COMMUNICATION IN INDIA DR. SUPARNA DUTTA, CHANDER MOHAN & PARTHO ACHARYA	49
11.	A STUDY ON IDENTIFYING KEY HUMAN RESOURCE MANAGEMENT PRACTICES AFFECTING ORGANIZATIONAL COMMITMENT OF ENGINEERS OF NCR SHEVATA SINGHAL, DR. SUNITA DWIVEDI & DR. MITU G. MATTA	53
12.	IMPACT OF LEADERSHIP ON PERFORMANCE: IN CONTEXT OF SCHOOL LEADERSHIP ADIL SOHAIL & RAJA MAZHAR HAMEED	59
13.	SERVICE QUALITY PERCEPTIONS: AN EMPIRICAL ASSESSMENT OF BANKS IN JAMMU & KASHMIR STATE DR. MUSHTAQ AHMAD BHAT, SUHAILA SIKEEN KHAN & AAJAZ AHMAD BHAT	65
14.	A STUDY ON INVESTORS' ATTITUDE TOWARDS STOCK MARKET INVESTMENT DR. R. AZHAGAIAH & K. BANUMATHY	70
15.	A COMPREHENSIVE MODEL TO CHECK THE ADOPTION OF ONLINE SHOPPING IN PAKISTAN MUHAMMAD RIZWAN, MUHAMMAD IMRAN, MUHAMMAD SAJID IQBAL, MUHAMMAD SAJID BHATTI, AQSA CHANDA & FOZIA KHANUM	78
16.	LASER COMMUNICATION SYSTEM KARTIKBHAI BALDEVBAHI PATEL	86
17.	PERCEPTION OF CUSTOMERS TOWARDS SMS MODE OF ADVERTISING: A STUDY AT WEST BENGAL DR. RITA BASU	95
18.	CUSTOMER RELATIONSHIP MANAGEMENT IN BANKING: ISSUES AND CHALLENGES DR. SARITA BHATNAGAR	99
19.	METHOD FOR DESIGN PATTERN SELECTION BASED ON DESIGN PRINCIPLES S. S. SURESH, SAGAR. S. JAMBHORKAR & ASHA KIRAN	103
20.	INVESTMENT OPPORTUNITIES OF SERVICE SECTOR IN INDIA DR. SEEMA SINGH & SARIKA AHLLUWALIA	108
21.	THE IMPACT OF CONTRIBUTORY PENSION SCHEME ON EMPLOYEE STANDARD OF LIVING OF QUOTED FIRMS IN NIGERIA SAMUEL IYIOLA KEHINDE OLUWATOYIN & DR. EZUGWU CHRISTIAN IKECHUKWU	113
22.	DETERMINANTS OF CUSTOMER COMPLAINING BEHAVIOR MUHAMMAD RIZWAN, AYESHA KHAN, IRAM SAEED, KAYNAT SHAH, NIDA AZHAR & WAQASIA ANAM	119
23.	A RELIABLE COMPUTERIZED ACCOUNTING INFORMATION SYSTEM; WHAT SECURITY CONTROLS ARE REQUIRED? AMANKWA, ERIC	125
24.	TRUST IN LEADERS - VITAL FOR EMPLOYEE MOTIVATION AND COMMITMENT: A CASE STUDY IN SELECTED CIVIL SERVICE BUREAUS IN AMHARA REGION, ETHIOPIA ABEBE KEBIE HUNEGNAW	132
25.	THE IMPACT OF ADOPTING COMPUTERIZED ACCOUNTING INFORMATION SYSTEMS FOR EFFECTIVE MANAGEMENT OF ACCOUNTING TRANSACTIONS IN PUBLIC INSTITUTIONS: CASE OF KENYA SCHOOL OF GOVERNMENT DUNCAN MOMANYI NYANGARA, THOMAS MOCHOGE MOTINDI & JAMES KAMAU MWANGI	138
26.	INCLUSIVE GROWTH THROUGH FINANCIAL INCLUSION: A STUDY OF INDIAN BANKING SECTOR SHRI LAXMIKANTA DAS & DR. SANJEEB KUMAR DEY	144
27.	A CONCEPTUAL MODEL FOR VENDOR SELECTION IN IT OUTSOURCING: AN APPROACH INSPIRED BY THE MONEYBALL THEORY DIANA LÓPEZ-ROBLEDÓ, EDGAR FERRER, MARIA LUGO-SALLS, JOSÉ BEAUCHAMP-COUTO & LEILA VIRELLA-PAGAN	147
28.	HOME LOAN FRAUDS- BANKER'S NIGHT MARE RAJU D	152
29.	ADVERSE EFFECT OF LOAN SECURITIZATION ON THE STOCK PRICES OF BANKS: EMPIRICAL EVIDENCE FROM EUROPE AND AMERICA SHARMIN SHABNAM RAHMAN	158
30.	ANTECEDENTS OF BRAND LOYALTY: AN EMPIRICAL STUDY FROM PAKISTAN MUHAMMAD RIZWAN, TAMOOR RIAZ, NAEEM AKHTER, GULSHER MURTAZA, M.HASNAIN, IMRAN RASHEED & LIAQUAT HUSSAIN	165
	REQUEST FOR FEEDBACK	172

CHIEF PATRON

PROF. K. K. AGGARWAL

Chancellor, Lingaya's University, Delhi
Founder Vice-Chancellor, Guru Gobind Singh Indraprastha University, Delhi
Ex. Pro Vice-Chancellor, Guru Jambheshwar University, Hisar

FOUNDER PATRON

LATE SH. RAM BHAJAN AGGARWAL

Former State Minister for Home & Tourism, Government of Haryana
Former Vice-President, Dadri Education Society, Charkhi Dadri
Former President, Chinar Syntex Ltd. (Textile Mills), Bhiwani

CO-ORDINATOR

DR. SAMBHAV GARG

Faculty, Shree Ram Institute of Business & Management, Urjani

ADVISORS

DR. PRIYA RANJAN TRIVEDI

Chancellor, The Global Open University, Nagaland

PROF. M. S. SENAM RAJU

Director A. C. D., School of Management Studies, I.G.N.O.U., New Delhi

PROF. S. L. MAHANDRU

Principal (Retd.), Maharaja Agrasen College, Jagadhri

EDITOR

PROF. R. K. SHARMA

Professor, Bharti Vidyapeeth University Institute of Management & Research, New Delhi

EDITORIAL ADVISORY BOARD

DR. RAJESH MODI

Faculty, Yanbu Industrial College, Kingdom of Saudi Arabia

PROF. PARVEEN KUMAR

Director, M.C.A., Meerut Institute of Engineering & Technology, Meerut, U. P.

PROF. H. R. SHARMA

Director, Chhatrapati Shivaji Institute of Technology, Durg, C.G.

PROF. MANOHAR LAL

Director & Chairman, School of Information & Computer Sciences, I.G.N.O.U., New Delhi

PROF. ANIL K. SAINI

Chairperson (CRC), Guru Gobind Singh I. P. University, Delhi

PROF. R. K. CHOUDHARY

Director, Asia Pacific Institute of Information Technology, Panipat

DR. ASHWANI KUSH

Head, Computer Science, University College, Kurukshetra University, Kurukshetra

DR. BHARAT BHUSHAN

Head, Department of Computer Science & Applications, Guru Nanak Khalsa College, Yamunanagar

DR. VIJAYPAL SINGH DHAKA

Dean (Academics), Rajasthan Institute of Engineering & Technology, Jaipur

DR. SAMBHAVNA

Faculty, I.I.T.M., Delhi

DR. MOHINDER CHAND

Associate Professor, Kurukshetra University, Kurukshetra

DR. MOHENDER KUMAR GUPTA

Associate Professor, P.J.L.N. Government College, Faridabad

DR. SAMBHAV GARG

Faculty, Shree Ram Institute of Business & Management, Urjani

DR. SHIVAKUMAR DEENE

Asst. Professor, Dept. of Commerce, School of Business Studies, Central University of Karnataka, Gulbarga

DR. BHAVET

Faculty, Shree Ram Institute of Business & Management, Urjani

ASSOCIATE EDITORS**PROF. ABHAY BANSAL**

Head, Department of Information Technology, Amity School of Engineering & Technology, Amity University, Noida

PROF. NAWAB ALI KHAN

Department of Commerce, Aligarh Muslim University, Aligarh, U.P.

ASHISH CHOPRA

Sr. Lecturer, Doon Valley Institute of Engineering & Technology, Karnal

TECHNICAL ADVISOR**AMITA**

Faculty, Government M. S., Mohali

FINANCIAL ADVISORS**DICKIN GOYAL**

Advocate & Tax Adviser, Panchkula

NEENA

Investment Consultant, Chambaghat, Solan, Himachal Pradesh

LEGAL ADVISORS**JITENDER S. CHAHAL**

Advocate, Punjab & Haryana High Court, Chandigarh U.T.

CHANDER BHUSHAN SHARMA

Advocate & Consultant, District Courts, Yamunanagar at Jagadhri

SUPERINTENDENT**SURENDER KUMAR POONIA**

CALL FOR MANUSCRIPTS

We invite unpublished novel, original, empirical and high quality research work pertaining to recent developments & practices in the area of Computer, Business, Finance, Marketing, Human Resource Management, General Management, Banking, Insurance, Corporate Governance and emerging paradigms in allied subjects like Accounting Education; Accounting Information Systems; Accounting Theory & Practice; Auditing; Behavioral Accounting; Behavioral Economics; Corporate Finance; Cost Accounting; Econometrics; Economic Development; Economic History; Financial Institutions & Markets; Financial Services; Fiscal Policy; Government & Non Profit Accounting; Industrial Organization; International Economics & Trade; International Finance; Macro Economics; Micro Economics; Monetary Policy; Portfolio & Security Analysis; Public Policy Economics; Real Estate; Regional Economics; Tax Accounting; Advertising & Promotion Management; Business Education; Management Information Systems (MIS); Business Law, Public Responsibility & Ethics; Communication; Direct Marketing; E-Commerce; Global Business; Health Care Administration; Labor Relations & Human Resource Management; Marketing Research; Marketing Theory & Applications; Non-Profit Organizations; Office Administration/Management; Operations Research/Statistics; Organizational Behavior & Theory; Organizational Development; Production/Operations; Public Administration; Purchasing/Materials Management; Retailing; Sales/Selling; Services; Small Business Entrepreneurship; Strategic Management Policy; Technology/Innovation; Tourism, Hospitality & Leisure; Transportation/Physical Distribution; Algorithms; Artificial Intelligence; Compilers & Translation; Computer Aided Design (CAD); Computer Aided Manufacturing; Computer Graphics; Computer Organization & Architecture; Database Structures & Systems; Digital Logic; Discrete Structures; Internet; Management Information Systems; Modeling & Simulation; Multimedia; Neural Systems/Neural Networks; Numerical Analysis/Scientific Computing; Object Oriented Programming; Operating Systems; Programming Languages; Robotics; Symbolic & Formal Logic and Web Design. The above mentioned tracks are only indicative, and not exhaustive.

Anybody can submit the soft copy of his/her manuscript **anytime** in M.S. Word format after preparing the same as per our submission guidelines duly available on our website under the heading guidelines for submission, at the email address: infoijrcm@gmail.com.

GUIDELINES FOR SUBMISSION OF MANUSCRIPT

1. **COVERING LETTER FOR SUBMISSION:**

DATED: _____

THE EDITOR
IJRCM

Subject: SUBMISSION OF MANUSCRIPT IN THE AREA OF

(e.g. Finance/Marketing/HRM/General Management/Economics/Psychology/Law/Computer/IT/Engineering/Mathematics/other, please specify)

DEAR SIR/MADAM

Please find my submission of manuscript entitled ' _____ ' for possible publication in your journals.

I hereby affirm that the contents of this manuscript are original. Furthermore, it has neither been published elsewhere in any language fully or partly, nor is it under review for publication elsewhere.

I affirm that all the author (s) have seen and agreed to the submitted version of the manuscript and their inclusion of name (s) as co-author (s).

Also, if my/our manuscript is accepted, I/We agree to comply with the formalities as given on the website of the journal & you are free to publish our contribution in any of your journals.

NAME OF CORRESPONDING AUTHOR:

Designation:

Affiliation with full address, contact numbers & Pin Code:

Residential address with Pin Code:

Mobile Number (s):

Landline Number (s):

E-mail Address:

Alternate E-mail Address:

NOTES:

- a) The whole manuscript is required to be in **ONE MS WORD FILE** only (pdf. version is liable to be rejected without any consideration), which will start from the covering letter, inside the manuscript.
- b) The sender is required to mention the following in the **SUBJECT COLUMN** of the mail:
New Manuscript for Review in the area of (Finance/Marketing/HRM/General Management/Economics/Psychology/Law/Computer/IT/Engineering/Mathematics/other, please specify)
- c) There is no need to give any text in the body of mail, except the cases where the author wishes to give any specific message w.r.t. to the manuscript.
- d) The total size of the file containing the manuscript is required to be below **500 KB**.
- e) Abstract alone will not be considered for review, and the author is required to submit the complete manuscript in the first instance.
- f) The journal gives acknowledgement w.r.t. the receipt of every email and in case of non-receipt of acknowledgment from the journal, w.r.t. the submission of manuscript, within two days of submission, the corresponding author is required to demand for the same by sending separate mail to the journal.

2. **MANUSCRIPT TITLE:** The title of the paper should be in a 12 point Calibri Font. It should be bold typed, centered and fully capitalised.

3. **AUTHOR NAME (S) & AFFILIATIONS:** The author (s) **full name, designation, affiliation (s), address, mobile/landline numbers**, and **email/alternate email address** should be in italic & 11-point Calibri Font. It must be centered underneath the title.

4. **ABSTRACT:** Abstract should be in fully italicized text, not exceeding 250 words. The abstract must be informative and explain the background, aims, methods, results & conclusion in a single para. Abbreviations must be mentioned in full.

5. **KEYWORDS:** Abstract must be followed by a list of keywords, subject to the maximum of five. These should be arranged in alphabetic order separated by commas and full stops at the end.
6. **MANUSCRIPT:** Manuscript must be in **BRITISH ENGLISH** prepared on a standard A4 size **PORTRAIT SETTING PAPER**. It must be prepared on a single space and single column with 1" margin set for top, bottom, left and right. It should be typed in 8 point Calibri Font with page numbers at the bottom and centre of every page. It should be free from grammatical, spelling and punctuation errors and must be thoroughly edited.
7. **HEADINGS:** All the headings should be in a 10 point Calibri Font. These must be bold-faced, aligned left and fully capitalised. Leave a blank line before each heading.
8. **SUB-HEADINGS:** All the sub-headings should be in a 8 point Calibri Font. These must be bold-faced, aligned left and fully capitalised.
9. **MAIN TEXT:** The main text should follow the following sequence:

INTRODUCTION**REVIEW OF LITERATURE****NEED/IMPORTANCE OF THE STUDY****STATEMENT OF THE PROBLEM****OBJECTIVES****HYPOTHESES****RESEARCH METHODOLOGY****RESULTS & DISCUSSION****FINDINGS****RECOMMENDATIONS/SUGGESTIONS****CONCLUSIONS****SCOPE FOR FURTHER RESEARCH****ACKNOWLEDGMENTS****REFERENCES****APPENDIX/ANNEXURE**

It should be in a 8 point Calibri Font, single spaced and justified. The manuscript should preferably not exceed **5000 WORDS**.

10. **FIGURES & TABLES:** These should be simple, crystal clear, centered, separately numbered & self explained, and **titles must be above the table/figure. Sources of data should be mentioned below the table/figure.** It should be ensured that the tables/figures are referred to from the main text.
11. **EQUATIONS:** These should be consecutively numbered in parentheses, horizontally centered with equation number placed at the right.
12. **REFERENCES:** The list of all references should be alphabetically arranged. The author (s) should mention only the actually utilised references in the preparation of manuscript and they are supposed to follow **Harvard Style of Referencing**. The author (s) are supposed to follow the references as per the following:
 - All works cited in the text (including sources for tables and figures) should be listed alphabetically.
 - Use **(ed.)** for one editor, and **(ed.s)** for multiple editors.
 - When listing two or more works by one author, use --- (20xx), such as after Kohl (1997), use --- (2001), etc, in chronologically ascending order.
 - Indicate (opening and closing) page numbers for articles in journals and for chapters in books.
 - The title of books and journals should be in italics. Double quotation marks are used for titles of journal articles, book chapters, dissertations, reports, working papers, unpublished material, etc.
 - For titles in a language other than English, provide an English translation in parentheses.
 - The location of endnotes within the text should be indicated by superscript numbers.

PLEASE USE THE FOLLOWING FOR STYLE AND PUNCTUATION IN REFERENCES:**BOOKS**

- Bowersox, Donald J., Closs, David J., (1996), "Logistical Management." Tata McGraw, Hill, New Delhi.
- Hunker, H.L. and A.J. Wright (1963), "Factors of Industrial Location in Ohio" Ohio State University, Nigeria.

CONTRIBUTIONS TO BOOKS

- Sharma T., Kwatra, G. (2008) Effectiveness of Social Advertising: A Study of Selected Campaigns, Corporate Social Responsibility, Edited by David Crowther & Nicholas Capaldi, Ashgate Research Companion to Corporate Social Responsibility, Chapter 15, pp 287-303.

JOURNAL AND OTHER ARTICLES

- Schemenner, R.W., Huber, J.C. and Cook, R.L. (1987), "Geographic Differences and the Location of New Manufacturing Facilities," Journal of Urban Economics, Vol. 21, No. 1, pp. 83-104.

CONFERENCE PAPERS

- Garg, Sambhav (2011): "Business Ethics" Paper presented at the Annual International Conference for the All India Management Association, New Delhi, India, 19-22 June.

UNPUBLISHED DISSERTATIONS AND THESES

- Kumar S. (2011): "Customer Value: A Comparative Study of Rural and Urban Customers," Thesis, Kurukshetra University, Kurukshetra.

ONLINE RESOURCES

- Always indicate the date that the source was accessed, as online resources are frequently updated or removed.

WEBSITES

- Garg, Bhavet (2011): Towards a New Natural Gas Policy, Political Weekly, Viewed on January 01, 2012 <http://epw.in/user/viewabstract.jsp>

A RELIABLE COMPUTERIZED ACCOUNTING INFORMATION SYSTEM; WHAT SECURITY CONTROLS ARE REQUIRED?

AMANKWA, ERIC
LECTURER
PRESBYTERIAN UNIVERSITY COLLEGE
GHANA


ABSTRACT

The objective of this study is to explore security controls that can be integrated into the design, development and implementation of the Computerized Accounting Information Systems to ensure information reliability and to propose an effective framework for categorizing Security Controls towards the attainment of information reliability. A critical literature review and empirical study using field observations and personal interviews were used to gather data, which was then analyzed and modelled, using Structured Analysis and design models to reflect security controls identified for implementation in the Computerized Accounting Information Systems. Schwartau's Time Base security model therefore presented an effective framework for categorizing identified controls. The results of the study however indicated that, three categories of security controls, which are Preventive controls (Access Control, Authentication, Authorization, Input (Data Entry) Control, and Cryptographic mechanism), Detective controls (Non-repudiation, Anti-Virus Programs, Information Integrity Control, Impersonation Control, and Analysis of Security Audit logs) and Corrective controls (Database Recovery control, and Application Recovery control) are essential for ensuring the reliability of information generated from CAIS. Accordingly, it was recommended to implement security controls in an integrated fashion to create multiple layers of security and to sensitize users at all levels on the need and importance of having controls in a Computerized Accounting Information Systems.

KEYWORDS

Computerized Accounting, Security Controls, Information Reliability, Controls Categorization.

INTRODUCTION

omputerized Accounting Information System defined as a computer-based system that processes financial information and supports decision making in the context of coordination and control of organizational activities (Sajady et al., 2008); is designed to keep track of all payments for strategic financial decision making.

Computerized Accounting Information System (CAIS) encounters serious security threats that may arise from the weakness of their security controls or from the nature of the competitive environment as the need for information is greater (Hayale and Khadra, 2006). At the same time, the very survival of organization depends on correct management, security and confidentiality of their information (Eduardo and Marino, 2004), since information assets constitute a significant proportion of an entity's market value (ITGI, 2001). Consequently security threats related to CAIS require a great attention from auditors and accountants in order to be recognized and minimized by evaluating organization security controls (Greenstein and Vasarhelyi, 2000). Several professional committees, such as AICPA that published SAS No.94 in 2001, have undertaken this endeavour, even though it was late. However, these initiatives were in the form of general instructions, and nothing specific viewed to be considered as detailed guidance to the auditors in their work, (Boynton, 2001; Kinusn, 2002).

In 2002, the Sarbanes-Oxley act called for "real time" disclosure of information on material changes in the financial conditions or operations of publicly held companies. As a result, organizations are more concerned with timeliness and quality of financial performance information (Uday, 2004). In view of these, the responsibility has increased dramatically on the accounting profession and information systems auditors, to quickly recognize and assess the risks that are associated with Computerized Accounting Information Systems in the IT environment and define detailed security controls framework to be maintained. This paper therefore identifies Security Controls (SC) that can be integrated into the design, development and implementation of CAIS to ensure information reliability. The study also aims to propose an effective and working framework for categorizing CAS security controls towards the attainment of information reliability.

LITERATURE REVIEW

A Security Control is a system that prevents, detects or corrects unlawful events in an organization. The purpose of a security control is to reduce losses (risks) by lowering likelihood of occurrence or by reducing the impact after a risk has occurred.

A growing body of research indicates that the existence and adequacy of security controls to protect Computerized Accounting Information System (CAIS) implemented in Institutions of Higher Learning (IHL) is essential for the assurance of confidentiality, integrity and continuous availability of vital information for business continuity. The adequacy of security controls in this research is therefore defined as the ability of implemented security controls to ensure confidentiality, integrity, and availability of information to support managerial decision making. *Confidentiality* means security controls must prevent the disclosure of information to unauthorized individuals or systems; *Integrity* means that controls must prevent unauthorized modification of information and *Availability* means that implemented controls of CAIS must ensure prevention of unauthorized withholding of information or resources (Gollman, 2006). In other words implemented controls must not deny authorised users access to information.

Section 302 of the Sarbanes-Oxley Act requires the CEO and the CFO to certify that the financial statements fairly present the results of the company's activities and requires them to certify that they have evaluated the effectiveness of the organization's internal controls. Security is a key component of internal control and systems reliability. The Trust Services Framework developed by the AICPA and the Canadian Institute of Chartered Accountants addresses a subset of the issues covered by COBIT, focusing specifically on five aspects of information systems controls and governance that most directly pertain to systems reliability: Security, Confidentiality, Privacy, Processing Integrity, and Availability.

Buttross and Ackers (1990) conducted a theoretical study in which they discussed microcomputer security exposure and microcomputer organizational, hardware, software and data security controls. Their study provided security controls checklist that could be used to help the internal auditors in evaluating computer security. Some of these security controls were selected for implementation in this study.

Henry (1997) carried out a survey on 261 companies in the US, to determine the nature of their accounting systems and security in use. Seven basic security methods were presented in his study. These methods were encryption, password access, backup of the data, viruses' protection, and authorization for system changes, physical system security and periodic audit. Relevant controls from this study were selected for implementation in this study.

Another study, carried out by Qurashi & Siegel (1997), assured the accountant's responsibility to check the security of the computer system. The researchers carried out a theoretical study to develop a security checklist. This list covers the following four security controls groups, which are Client policy, Software security, Hardware security and Data security.

The IT Governance Institute (ITGI) and the Information Systems Audit and Control Foundation (ISACA) (1992) 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. Many of the COBIT security controls were selected and incorporated in the proposed security controls to be empirically tested in the CAIS environment at the PUCG.

Moscove and Stephan (2001) consider that e-business organizations should maintain a group of control procedures to protect their systems from any possible threats, such procedures includes:

1. Physical access control procedures.
2. Password control procedures.
3. Data encryption such as public key encryption.
4. Disaster recovery plan (DRP).
5. Software-based security control, such as firewalls.
6. Intrusion detection software to detect unauthorized entrance into the system

In a study carried out by Zviran and Haga (1999) to evaluate password security as one of the most common control mechanisms for authenticating users of CAIS, it was found that despite the widespread use of passwords, little attention has been given to the characteristics of their actual use. The study investigated the core characteristics of user-generated passwords and the associations among those characteristics.

Abu Musa (2006) also performed an empirical study to investigate and evaluate the existence and adequacy of implemented CAIS security controls in Saudi organizations using a proposed security controls checklist. The proposed security controls check list included; organizational controls, hardware and physical access control, software control, data security control and off-line data and program security control.

Drawing upon Abu-Musa (2006), Microsoft Corporation (2006) took the study a step further and categorized security controls under Organizational, Operational and Technological controls, with each of the categories consist of preventative controls, detection controls and management controls.

In a very recent publication, SANS Cyber Defense (2010) presented a Consensus Audit Document stating the Twenty Critical Security Controls for effective cyber defense. These Top 20 Controls were agreed upon by a powerful consortium brought together by John Gilligan (previously CIO of the US Department of Energy and the US Air Force) under the auspices of the Center for Strategic and International Studies. Members of the Consortium include NSA, US Cert, DoD JTF-GNO, the Department of Energy Nuclear Laboratories, Department of State, DoD Cyber Crime Center plus the top commercial forensics experts and pen testers that serve the banking and critical infrastructure communities. Security controls presented included;

1. Inventory of Authorized and Unauthorized Devices
2. Inventory of Authorized and Unauthorized Software
3. Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers
4. Boundary Defense
5. Maintenance, Monitoring, and Analysis of Security Audit Logs
6. Application Software Security
7. Controlled Use of Administrative Privileges
8. Controlled Access Based on Need to Know
9. Continuous Vulnerability Assessment and Remediation
10. Malware Defenses

IMPORTANCE OF THE STUDY

The study has the significance of reducing accounting related losses by presenting security controls necessary for achieving organizational pre-defined control objectives. From a practical standpoint, IS developers, Auditors, IT users and practitioners alike stand to gain from the findings of this study. The results could enable them to better understand and secure their CAIS and to champion IT development for the success of their businesses. While there have been several studies on information security controls implementation in Organizations in Europe and other parts of the world, very limited (if not zero) studies have been conducted on African organizations, hence this study bridges the existing research gap. It is also imperative to realize that all previous studies on the subject only identified generic information security controls, with few on accounting systems but failed to show how these controls can be integrated into the general design and implementation of accounting systems to achieve information reliability. The researcher at the time of this research was also unaware of any studies that identified security controls for direct integration into the design, development and implementation of computerized Accounting Systems. Hence the results of this study can provide valuable insights for CAIS developers, accountants and IS auditors, and lead to a better understanding of design and development issues concerned with security controls implementations in CAIS.

STATEMENT OF THE PROBLEM

In view of the above this study attempts to answer the following questions: (1). *what security controls are necessary for ensuring the reliability of information generated from Computerized Accounting Information Systems (CAIS)?* (2). *which framework is effective for categorizing CAIS security controls to achieve information reliability?*

OBJECTIVES

The study strives to achieve the following objectives; (1).To identify security controls for direct integration into the design, development and implement of CAIS. (2). to propose an effective and working framework for categorizing CAS security controls towards the attainment of information reliability.

RESEARCH METHODOLOGY

This study was conducted at the Presbyterian University College Ghana, a private university with a student population of about 1,500 and total staff strength of about 200. The college has a well equipped accounts department headed by the college's finance director. All cash inflows and outflows within the college are solely handled by the college's finance department which is equipped with computerized accounting information system (CAIS) developed in-house and used on all its campuses, thus, making it an appropriate case for this study. The department maintains several books of accounts for the college, notable ones include, assets, payroll, petty cash, fees payment and others. However, in order to ensure a comprehensive study into the operations of the department, two of these accounts (Fees-payment and Payroll) are used to show how security controls can be integrated to ensure information reliability in these accounts, since the same process can be replicated in all other accounts in the college. These accounts were selected for analysis because the core business of the college's accounts department is to collect fees (revenue) and pay salaries (expenditure) to employees.

The research design chosen for this research is the exploratory. The choice of qualitative method of data collection including interviews and observation is largely guided by the unstructured nature of the research question "what security controls are necessary for ensuring the reliability of information generated from Computerized Accounting Information Systems (CAIS)". The qualitative method was used because it allowed the researcher to gain a qualitative understanding of the underlying reasons to the problem using a small sample size and non-statistical data analysis to develop an initial in-depth understanding of or solution to the problem.

The study starts with a critical review of existing literature on accounting information systems and security controls so as to identify generic security controls possible for implemented in computerized accounting system, and to identify an effective model for categorizing these controls. Empirical results from existing literature and previous studies (Abu-Musa (2006), Microsoft (2006), Buttross and Ackers (1990), Zviran and Haga (1999), Henry (1997), SANS (2010), Sarbanes-Oxley Act and COBIT (2005)) were reviewed for the identification of generic security controls. However, to categorize the identified security controls towards the assurance of information reliability, Schwartau's (1999) Time Based Security model which categorized controls into preventive, detective and reactive was used. The model was selected as effective for achieving this goal due to its ability to show the relationship between security controls and their effect on information reliability.

Questions for interviews and artefacts for observation were also formulated based on existing literature. After a careful consideration of selected questions and artefacts, two rounds of separate interviews were conducted to; (1) gather requirements for the development of a new system; and (2) ascertain the existence and effectiveness of security controls identified at the PUCG. Existing accounting system (Fees payment & payroll accounts) at the PUCG was then analyzed to identify functional and non-functional requirements for the development of an accounting system. Model-driven approach which emphasizes the drawing of pictorial system models to document and validate a system was employed for analyzing the existing accounting system at the PUCG. The existing fee-payment and payroll accounts selected for the study were modelled using flowchart for subsequent analysis and investigations. This gave the researcher a perfect idea of the existing business processes which served as guide for designing a new system.

This was succeeded by a design of a new accounting system equipped with the carefully selected security controls for integration and implementation based on functional requirements and framework adopted during the literature review. Flowcharts again served as the tool for creating the new design. The new design was then implemented with a selected programming language (Visual Basic 2008), database management system (MySQL 5.0) and cryptographic mechanisms (encryption algorithm – blow fish and hash function – MD5 influenced by the fact that, no attack has been discovered to be successful on these cryptographic mechanisms as of the time of this research (BrightHub, 2010)).

To evaluate the newly developed system, users at the PUCG were divided into direct users and indirect users. Direct users are those users who use the system in their day to day operations at the college whereas indirect users are those who benefit from information generated from the system for decision making. Interview with Direct users helped to capture functional and non-functional requirements. A self administered questionnaire was used to evaluate the acceptability of the new system in two main areas – that is functional requirement acceptability and security controls acceptability. Ten users from the PUCG who interact directly or indirectly with the accounting system were selected for this purpose. These users included the President of the College, Finance director, College registrar, Accountant and Accounting Assistant, internal auditor and Assistant, Network Administrator and two accounts clerks. The questionnaire was made up of two sections (Functional requirements and Security controls) with a total of six open ended questions. Data gathered was categorized using the two section, was reduced and eventually interpreted for conclusion to be drawn.

FINDINGS/RESULTS AND DISCUSSIONS

The study sets out with the objective to identify Security Controls (SC) that can be integrated into the design, development and implementation of Computerized Accounting Information Systems (CAIS) to ensure information reliability. This was to be achieved through a critical review of existing studies and empirical studies on the Presbyterian University College Ghana (PUCG).

A careful analysis performed on the data collected from the Presbyterian University College Ghana (PUCG) Accounting System (through interviews and observations) to identify requirements (functional and non-functional) for the development of the proposed system, showed that the PUCG had implemented **physical security** and **Authentication** (username and password) as preventive controls but inadequately implemented; as usernames and passwords are stored in plaintext in the database. There was also no mechanism to hold users accountable for their actions (**Non-repudiation**). There were no **Access Controls** as a user could access any part of the system without any restrictions. Sensitive financial information was also stored in plaintext without any **Encryption** in the database. **Periodic backups** at remote locations which would return the system back to its normal operation should any error occur was also not present. Finally, information confidentiality, and integrity was also not ensured. The absence these security controls therefore made information generated less useful and reliable for decision making at the PUCG.

After the implementation of the new design at the Presbyterian University College Ghana (PUCG), a usability evaluation was carried out to ensure the ease of acceptability of the new system (Security Enhanced CAIS). The evaluation was based on the categorization presented in the CAIS security control model developed. The usability evaluation indicated that Indirect users (top management) showed a more positive attitude and exhibited immense understanding and concerns towards implementation of security controls in a CAIS whereas direct users showed very little understanding and concern on the need for security controls in CAIS.

Various researchers have in the past presented security controls for ensuring information reliability but only a few have direct relationship with Accounting systems, notable ones are Abu-Musa (2006), Microsoft (2006), Buttross and Ackers (1990), Zviran and Haga (1999), Henry (1997), SANS (2010), Sarbanes-Oxley Act and COBIT (2005). Based on existing literature and the empirical study conducted on the PUCG Accounting System, the following Security Controls, presented in tabular form, were identified as effective for direct integration into the design, and implementation of Computerized Accounting Information System. These security controls are summarized and described in the table below:

TABLE 1: SECURITY CONTROLS

SECURITY CONTROLS	DESCRIPTION
1. User Access Control	This is a mechanism for restricting access to certain information based on a user's identity and membership in various predefined groups
2. Authentication	Authentication is the process of verifying a claim of identity.
3. Authorization	Determining what informational resources users are permitted to access and what actions they will be allowed to perform.
4. Input (Data Entry) control	Data entry errors arising from human negligence
5. Cryptographic mechanism	The use of cryptographic mechanisms such as encryption, hashing and digital signatures to ensure information confidentiality and integrity.
6. Database Recovery Control	This controls ensures that the systems restores to normal operation after an error has occurred, using a remote backup of the database.
7. Application Recovery Control	A control to ensure timely repair of all corrupt application using backups on removable media.
8. Analysis of Security Audit Logs	A control to monitor and track system behaviour that deviates from expected norms
9. Impersonation Control	This security control is used to detect masquerades mounted on the system.
10. Information Integrity Control	A control to determine any compromise in the database. It determines whether unauthorized changes have been made to information stored in the database.
11. Anti-Virus Programs	An application software to detect and respond to malicious software, such as viruses and worms
12. Non-Repudiation	A Security control to ensure that a user performing an action in the Computerized Accounting System cannot falsely deny that he or she performed that action

The table above (table 1) shows the results from the critical literature review and the empirical studies conducted on the Accounting System at the Presbyterian University College Ghana to identify security controls which can be integrated into the design, development and implementation of Computerized Accounting Systems to ensure information reliability.

These security controls are discussed below:

User Access Control: This is a mechanism for restricting access to certain information based on a user's identity and membership in various predefined groups (Microsoft, 2006). In this study, user access control was found to be a mechanism for ensuring that, users in the CAS environment are allowed access, only to

information for which they are authorized to access; thus ensuring confidentiality and integrity of information. However, the sophistication of the access control mechanisms should be in parity with the value of the information being protected - the more sensitive or valuable the information the stronger the control mechanisms need to be. Access control is essential for ensuring information reliability, therefore every user of the CAIS must be assigned an Access Level by the System Administrator and this Access Level must determine the privileges to be enjoyed by the user. This therefore helps in ensuring segregation of duties as various users are assigned various roles based on their access rights, hence information reliability is achieved. User access control is essential for ensuring information reliability, in that access control seeks to prevent activities that could lead to a breach of security (Sandhu and Samarati, 1994) and provides administrators with the capability to regulate who can perform what action, where and when, in what order and in some cases under what relational circumstances (NIST, 1998; Baker and Grosse, 1995).

User Authentication: authentication is an essential security control for ensuring the reliability of information generated from CAIS, and its relevance cannot be understated. Authentication is the process of verifying a claim of identity. 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. Most commonly authentication establishes the identity of a user to some part of the system, typically by means of a password. More generally, authentication can be computer-to-computer or process-to-process and mutual in both directions. Authentication must require that the person, process, or device making the request provides a credential that proves it is what or who it says it is. For example, in the CAIS environment, users must provide identification and authentication key (two way authentication) for the system to verify. Whenever a user enters his identification (say e.amankwa – a claim of identity), the system requests for an authentication key (a secret code known to only the user) and then scans its database to find a match. If it finds a match, then the user is authenticated and is therefore granted access into the system else access is denied. This security control helps in ensuring that only authorized users are allowed into the CAIS and is effective for ensuring accountability and reliability in the CAIS environment. It is also imperative to know that users' identification (usernames) and authentication codes (passwords) used in this study were hashed with the message digest five (MD5) cryptographic hash function to ensure that any attack on the communication medium or on the database to retrieve usernames and passwords proved futile. Authentication enables organizations to provide secure access to digital data and applications thereby save significant costs in their ongoing business activities. Costs incurred through information leakages such as court fines, and investigations are avoided.

However, the human aspect of the CAIS made it difficult to implement authentication. In this study users comprised both the young and the aged with several responsibilities within the institution. Such users for fear of forgetting their passwords write them in their diaries and on stickers for future reference. This therefore compromises the security policies and controls introduced in the system and thereby reduce information reliability.

User Authorization: After a user has successfully been identified and authenticated then it must be determined what informational resources they are permitted to access and what actions they will be allowed to perform (print, view, create, delete, or change); this is called Authorization. Authorization is the process of assuring that users have access to the functionality and information that they require and no more. In this study authorization is derived from the identity of a user, authentication key and access level as assigned by the system administrator. Aspects of the system to be accessed by the different access-levels created were based on business rules that exist in the PUCG. This rule permitted users at access-level 1 to access all parts of the system, where level 2 could access also access all parts except the creation of new user accounts and system configuration. Level 3 users on the other hand could only enter data into accounts.

Cryptographic Mechanism: Cryptography is used to transform usable accounting information into a form that renders it unusable by anyone other than an authorized user. The most frequently applied Cryptographic schemes are; Encryption algorithms, Digital signatures and Cryptographic hash functions (Gollmann, 2006). Cryptographic mechanisms used in the CAIS environment include Encryption and hash functions. Although several encryption algorithms exist, the Blowfish algorithm which is symmetric (uses a single key for encryption and decryption) was selected for implementation due to its strength over other algorithms. No attack has been discovered to break the blowfish encryption (BrightHub, 2010), and this simply means that once sensitive information for strategic decision is encrypted no unauthorized user can tamper with it; hence reliability is guaranteed. However due to the symmetric nature of the blowfish algorithm, its strength is highly dependent on the secrecy of the encryption key (password or pass-phrase for encrypting information) in the CAIS environment. The responsibility information reliability is shifted from the users and now rests with the programming team who must be held accountable for any compromise.

Input Controls (Data Entry): this refers to data entry errors which have the potential of reducing the reliability of accounting system information. The CAIS must therefore ensure that all data entered are validated correctly before update. For example the system must ensure that data entered for numeric textboxes are numeric values and not string values, as this may lead to unexpected results and sometimes system crash

Non-Repudiation: The technique used to ensure that someone performing an action on a computer cannot falsely deny that he or she performed that action. Non-repudiation provides undeniable proof that a user took a specific action such as transferring money, altering payroll figure, or printing a report. In a CAIS an internal audit log is used for ensuring non-repudiation. Information such as username, date, time and operations performed by every user of the system is automatically captured into the system's log file for future auditing. This helps to ensure proper accountability within the CAIS environment and eventually leading information reliability.

Anti-Virus Programs: Designed to detect and respond to malicious software, such as viruses and worms. Anti-virus software provides a comprehensive security for the CAIS environment. They can be signature-based or heuristics-based or both. In signature-based antivirus, signature files are developed by security vendors to prevent and detect known threats. Although this is very common on the market today, it is prone to zero-day attack (an attack that exploits the vulnerabilities in an application before it becomes known to the developer) due to the numerous sophisticated tools available to virus writers. Heuristics-based anti-virus software on the other hand analyzes the behaviour of codes on access and intercepts possible threats before execution. Heuristics-based anti-virus reports threats based on suspicions and often results in false-positive. In view of these setbacks an anti-virus solution for the CAIS environment must combine both heuristics and signature files and must be updated at frequent intervals to ensure optimal protection against known and emerging threats.

Information Integrity Control: Makes it possible for system administrators and information systems auditors to determine whether unauthorized changes have been made to information stored in the database. For example a cryptographic hash function such as message digest five (MD5) can be used to hash all sensitive financial information and be stored in temporary database table. Whenever information is retrieved from the operational database table, it must be subjected through the same hash function and after compare the current and previous hash values of the retrieved information. If the two are in agreement then it means information integrity has not been compromised and is therefore reliable for strategic business decision making. However if the previous is different from the current then it means that unauthorized changes have occurred and this must be investigated by analyzing the security audit log to determine the author, date and time stamps of the changes.

Impersonation Control: this security control is used to detect masquerades mounted on the system. This control is triggered automatically when an unauthorized user tries to log into the system with the identity of an authorized user. The effectiveness of this control is achieved programmatically by blocking or suspending user accounts which failed to authenticate for three consecutive times. Owners of such user accounts must inform the system administrator for their user accounts to be activated again. This helps to ensure that only authorized users are granted access into the system and thereby enhance the reliability of information.

Analysis of Security Audit Logs: this control makes it possible to monitor and track system behaviour that deviates from expected norms. It helps in detecting, understanding, and recovering from security breaches. An internal security audit log introduced at every operation part of the CAIS records details of users' actions such as operation performed, date, time and username. This information can help in detecting and correcting system breaches when provided for analysis on time. In view of this, this control help in presenting the most recent operations recorded in the audit log in three days interval by automatically sending a print command to printer connected to the administrator or auditor's computer. To ensure such vital information does not get into the hands of unauthorized users, users' access level is considered before sending the command. As a result, security breaches are detected and corrected on time.

Database Recovery Control: this control requires backup systems to be made at offsite locations to facilitate the restoration of lost or corrupted data. In the event of a catastrophic incident, backup media stored offsite makes it possible to store critical business data on replacement systems. This control helps to ensure availability of information in the CAIS environment at all time.

Application Recovery Control: This control requires that copies of application setup for installation and repair be kept on removable storage devices to restore the system back into operation in the event the one in use corrupts or malfunctions. This control helps to ensure availability of the system and subsequently information for timely decision making.

However, in an attempt to identify an effective scheme for classifying those security controls which can be integrated into the design, development and implementation of CAS, the study also found that three (3) categories of Security Controls are needed for ensuring the reliability of information generated from CAIS.

A study conducted by Hayle & Khadra (2006) to evaluate the level of Control Systems effectiveness in Computerized Accounting Information Systems (CAIS) that is implemented in the Jordanian banking sector to preserve confidentiality, integrity and availability of the bank's data and their CAIS categorized CAIS security controls according to their functions under the following;

1. Fraud and error reduction control.
2. Physical access.
3. Logical access.
4. Data security controls.
5. Documentation standards.
6. Disaster Recovery Plan.
7. Internet, communication and e-banking controls.
8. Output security controls.

Abu Musa (2006) in study to investigate and evaluate the existence and adequacy of implemented CAIS security controls in Saudi organizations, categorized CAIS security controls under Organizational security controls, hardware and physical access control, software control, data security control and off-line data and program security control.

Microsoft Corporation (2006) on the other hand, categorized security controls under Organizational Controls, Operational Controls and Technological controls; with each of the categories consist of preventative controls, detection controls and management controls.

Buttross and Ackers (1990) in their study in which they discussed microcomputer security practice, categorized security controls under Organizational controls, Hardware controls, Software controls, Data and data integrity controls.

Schwartau's (1999) Time Based Security (TBS) model categorizes security controls under preventive controls, detective and corrective (reactive) controls. The model focuses on the relationship between preventive, detective and corrective controls and evaluates the effectiveness of an organization's security by measuring and comparing the relationship among them. That is, if the time it takes an attacker to break through the organization's preventive controls is greater than the sum of the time it takes to detect that an attack is in progress and the time it takes to respond to the attack, then the organization's security procedures are effective. However, if the time it takes an attacker to break through the organization's preventive controls is less than the sum of the time it takes to detect that an attack is in progress and the time it takes to respond to the attack, then the organization's security procedures are ineffective. Hence information is unreliable. Using Schwartau's (1999) Time Based Security (TBS) model the following is expressed:

P_t = the time it takes an attacker to break through the organization's preventive controls

D_t = the time it takes to detect that an attack is in progress

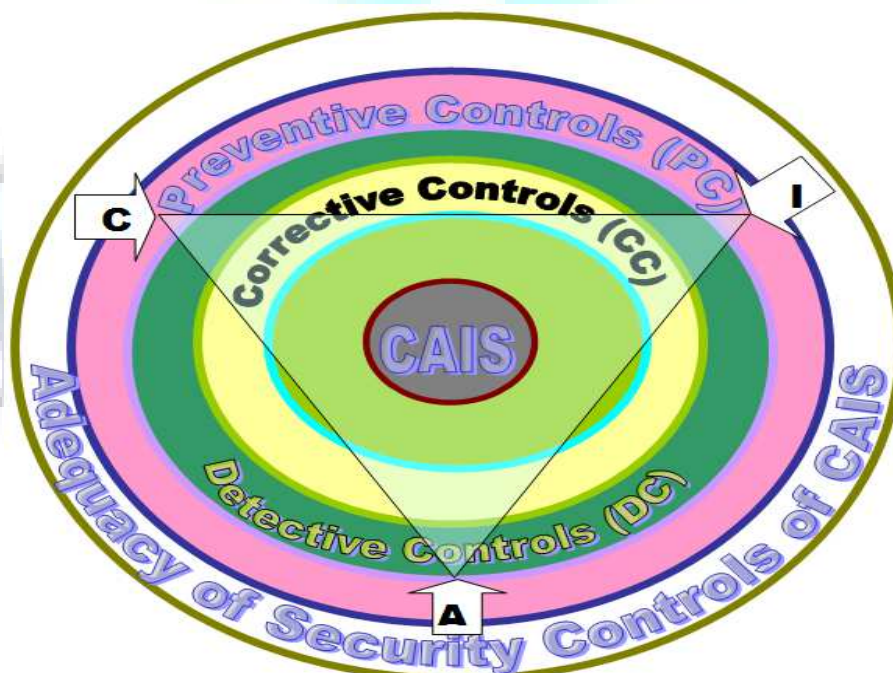
C_t = the time it takes to respond to the attack

If $P_t > D_t + C_t$, then the organization's security procedures are effective.

If $P_t < D_t + C_t$, then the organization's security procedures are ineffective

Based on the components of the TBS model above, security controls are categorized in this study under Preventive (P_c), Detective (D_c) and Corrective controls (C_c). However, to achieve information reliability, Confidentiality, Integrity, and Availability (CIA) which are essential components for achieving an organization's business and governance objectives over IT resources (COBIT & the Trust Services framework) were selected to develop a model for implementing Security Controls in the Computerized Accounting Information System (CAIS). These components therefore enforce multiple layers of controls in order to avoid having a single point of failure. Multiple Security Control layers increases effectiveness and thus information reliability because even if one procedure fails or is circumvented, another may function as planned. Security Controls, (categorized under Preventive, Detective and Corrective controls) together with the other information security components (CIA) are modelled to show how each layer offers protection to achieve Information Reliability (IR) in the CAIS environment. This conceptual model is shown in Figure 1 below.

FIGURE 1: CAIS SECURITY CONTROL CONCEPTUAL MODEL



The conceptual mode above (figure 1) expresses the relationship between the three categories of security controls identified. As Security Controls (SC) restricts access to authorized user only; it also ensures that, the confidentiality (C) of sensitive organizational information is protected; provides for processing Integrity (I) by preventing submission of unauthorized or fictitious transactions as well as preventing unauthorized changes to stored data or programs; and provides protection against a variety of attacks, including viruses and worms, thereby ensuring that the system is available (A) when needed.

Using Schwartz's (1999) Time Based Security (TBS) model, the CAIS security control model above (in figure 1) expresses two main relationship between CAIS information (Info), the time it takes an attacker to break through the organization's preventive controls (PC), the time it takes to detect that an attack is in progress (DC), the time it takes to respond to the attack (CC), confidentiality (C), Integrity (I) and Availability (A).

1. If $PC > DC + CC$, then $Info = C + I + A$, hence Info = reliable

2. If $PC < DC + CC$, then $Info \neq C + I + A$, hence Info = unreliable

The first case (1) expresses that if the time it takes an attacker to break through the organization's preventive controls is greater than the sum of the time it takes to detect that an attack is in progress and the time it takes to respond to the attack, then information generated from CAIS is said to be confidential, integrity maintained and available in a timely manner, hence information is reliable. However, if the time it takes an attacker to break through the organization's preventive controls is less than the sum of the time it takes to detect that an attack is in progress and the time it takes to respond to the attack (expressed in 2 above), then information generated from CAIS is said to be exposed, integrity compromised and unavailable to users, hence information is unreliable.

The table below (table 2) therefore shows the selected security controls for integration into the design and implementation of CAIS to ensure information reliability, classified under Preventive Controls, Detective Controls and Corrective Controls.

TABLE 2: CATEGORIZED CAIS SECURITY CONTROLS

PREVENTIVE CONTROLS (PC)	DETECTIVE CONTROLS (DC)	CORRECTIVE CONTROLS (CC)
Access Control	Non-repudiation	Database Recovery control
Authentication	Anti-Virus Programs	Application Recovery control
Authorization	Information Integrity Control	
Input (Data Entry) Control	Impersonation Control	
Cryptographic Mechanism	Analysis of Security Audit logs	

Since the continuous sustainability of an organization depends heavily on reliable financial information generated from accounting systems, which translates into strategic decisions, security controls are therefore required in such systems to prevent known and unknown events with the capability of preventing the organization from reaching its set objective. **Preventive controls** are therefore designed in Computerized Accounting Information Systems to arrest known error that may occur. However, unknown error that the system could not prevent and have occurred in the system must be detected as soon as possible for correction. SANS (2010) Cyber Defense states that "for those attacks that are successful, defenses must be capable of detecting, thwarting, and responding to follow-on attacks, as attackers spread inside a compromised system". Therefore, since Preventive Controls are never 100 percent in blocking all attacks, **Detective controls** are required in the CAIS environment to detect all error that might have bypassed preventive controls so as to ensure that decisions are not made based on the erroneous information from the system. **Corrective Controls** on the other hand involve the need for the system to react to incidents to take corrective actions on a timely basis. Many rely on human judgment. Planning and preparation are important. The system must eventually be restored after errors are detected and this can be achieved with the careful design and implementation of corrective controls in the CAIS.

The study's finding is therefore in agreement with Flowerday and Rossouw (2005) who identified preventive, detective and corrective controls as relevant for ensuring effectiveness of systems and integrity of information.

Since information is a major asset in organizations, and the continuous existence and sustainability dependent on information, any known incident with the potential to compromise the integrity of such vital information must be prevented from occurring. The existence of preventive controls means that the organization can make informed and reliable decisions and thus increase its information value. Costs incurred from investigating all such incidents are also avoided. However, since security is not a destination but a journey (Baker and Wallace, 2007) and hacking tools are growing fast ahead of security controls, provisions must be made to detect any case of incident occurrences in the CAIS. This helps to acknowledge the occurrence of errors and subsequently return the system to its normal operation.

The finding also corroborates that of Microsoft Corporation (2006) which classified each of the information system security controls under preventative, detection and management controls. COBIT's (2005) framework and Abu-Musa (2006) also agree with study's finding that, controls are needed to ensure more timely and reliable information from information systems. Although the finding replicates that by other researchers, the current study moves a step further by exploring implementation issues which were not considered in the previous studies. For example the current study points out specifics of security controls implementation in the CAIS environment; such as cryptographic mechanisms, programming language, database management system as well as the system architecture for implementing security control. The finding therefore has important implications for developing Computerized Accounting Information Systems in Institutions of Higher Learning.

CONCLUSIONS AND RECOMMENDATIONS

The main objective of this study was to investigate security controls necessary for ensuring the reliability of information generated from Computerized Accounting Information Systems (CAIS) and to propose a framework for categorizing CAIS security controls.

To achieve this, the proposed (12) security controls and classified in table 2 above need to be implemented in an integrated fashion as depicted in the CAIS security control model (in fig 1.0). This simply means that Preventive controls must be accompanied by Detective controls and subsequently Corrective controls. When CAIS security controls are implemented in an integrated manner, it would create multiple layers of security which increases effectiveness and ensures information reliability because even if one security layer fails or is circumvented, another may function as planned. Thus implementing Security Controls in an integrated fashion would contribute immensely towards the assurance of information reliability in the CAIS environment.

Cryptographic mechanisms must be used to aid implementation to achieve optimal protection. Cryptographic mechanisms including encryption, hash functions and digital signatures should be implemented as the final layer of the preventive controls. These mechanisms strengthen authentication procedures and play an essential role in ensuring and verifying the validity of CAIS transactions. There CAIS developers and designers need to understand cryptographic mechanisms to ensure proper integration and implementation.

According to Baker and Wallace (2007) "Security is not destination but a journey", therefore organizations must ensure periodic maintenance and upgrade of their computerized systems so as to prevent possible zero-day-attacks such systems. Since no system is full-proof, periodic maintenance and upgrade must be performed from time to time in order to solve all system errors detected to avoid future occurrences.

It is also imperative to know that, technical approaches alone can't solve all security problems for the simple reason that information security isn't merely a technical problem (Baker and Wallace, 2007), therefore in order to achieve information reliability in Computerized Accounting Systems, managerial policies and controls must equally be strengthened and users must also be sensitized on the relevance and need for controls to exist in CAIS through periodic training and workshops. People play a critical role in CAIS environment. Therefore, training is a critical preventive control as employees must understand and follow the organization's security policies. All employees should be taught why security measures are important to the organization's long-run survival. User of the CAIS must be abreast with current security threats to the entire organization and its inherent information. User must be trained on the need to enforce policies such as; never open unsolicited e-mail attachments, only use approved software, never share or reveal your passwords, and taking steps to physically protect laptops. Training is also needed to educate employees about social engineering attacks, which use deception to obtain unauthorized access to information resources. Executive support, Organizational and attitudinal change at all levels are essential for the successful implementation of a CAIS.

SCOPE FOR FURTHER RESEARCH

Further research could be undertaken to develop a value model for the implementation of security controls in CAIS, which would allow an in-depth analysis of the costs and benefits in a more organized way. The e3-value model can be used as tool for determining the actual economic value created by the implementation of security controls in CAIS. Further research is also needed to investigate the challenges in the implementation of security controls in Computerized Accounting Information systems in Institutions of Higher Learning in Ghana.

REFERENCES

1. Abu-Musa A. Ahmad (2006), evaluating the security controls of computerized accounting information systems in developing countries: the case of Saudi Arabia, *The International Journal of Digital Accounting Research* Vol. 6, p. 25-64.
2. AICPA, Auditing Standards Board. "SAS No. 94: The Effect of Information Technology on the Auditor's Consideration of Internal Control in a Financial Statement Audit". April 2001
3. Baker Wade H. and Wallace Linda (2007), "Is Information Security Under Control? Investigating Quality in Information Security Management", I EEE Computer Society – Security and Privacy, Virginia Tech press, US
4. Boynton W., Johnson R. and Kell W., "Modern Auditing", John Wiley & Sons Inc., Seventh edition, p322,400,401, 2001.
5. Bright Hub(2010) data encryption algorithm comparison [Online] Available at: <http://www.brighthub.com/computing/smb-security/articles/75099.aspx>, [Accessed on 30th April, 2011]
6. BUTTROSS, T.E.; ACKERS, M.D. (1990): "A Time - Saving Approach To Microcomputer Security", *Journal Of Accounting & EDP*, vol. 6, Iss. 1, pp.3135. – 35
7. Control Objective for Information and related Technology (COBIT), 4th Edition, (2005), COBIT FRAMEWORK 4.0, IT Governance Institute press, USA
8. Eduardo Frenandez-Medina and Marino Piattini, "Designing Secure Databases", *Information and Software Technology Journal*, Vol. 47, 2005.
9. Flowerday Stephen and Rossouw Von Solms (2005), Real-time information integrity=system integrity+data integrity+ continuous assurances, *Computers & Security*, Volume 24, Issue 8, Pages 604-613
10. Gollmann Dieter (2006), *Computer Security-2nd Ed.* John Wiley & sons Inc, England.
11. Hayale Talal H. and Khadra Husam A. Abu (2006), "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*, volume 13, pp. 39-68.
12. HENRY, L. (1997): "A Study of the Nature and Security of Accounting Information Systems: The Case of Hampton Roads, Virginia", *The Mid-Atlantic Journal of Business*, vol. 33, Iss. 63, pp.171-189.
13. ITGI (IT Governance Institute). IT governance executive summary; board briefing on IT governance. Rolling Meadows, 2001.
14. Kinsun Tam, "Implementing Internal Accounting Controls as Constrains in RDBMS and XML". Working paper European conference of AIS on 2002.
15. Microsoft Corporation (2006) information security controls - the security risk management guide [Online] Available at: <http://www.microsoft.com/Downloads/details.aspx?> [Accessed on 4th April, 2011]
16. Moscovice, Stephen A., "E-Business Security and Controls", *CPA Journal*, Vol. 71, Issue 11, Nov2001..
17. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (1998): Federal Computer Security Program, Managers' Forum Working Group, Guide for Developing Security Plans for Information Technology Systems, Special Publication 800-18, December
18. Presbyterian University College Ghana (2010), Handbook and Students Guide 2009 – 2011, Tyme Impression Ltd Ghana.
19. QURESHI, A.A.; SIEGEL, J.G. (1997): "The Accountant And Computer Security", *The National Public Accountant*, Washington, May, vol. 43, Iss. 3, pp. 12-15.
20. Sajady H., M. Dastgir, and H. Hashem Nejad, M. S. (2008), evaluation of the effectiveness of accounting information systems, *International Journal of Information Science & Technology*, Volume 6, Number 2.
21. SANS Cyber Defense (2010) 20 Critical Security Controls [Online] [Accessed on 5th November, 2010] Available at: <http://www.sans.org/critical-security-controls>
22. Schwartzau Winn (1999), "Time Based Security – Mesearing security and defensive strategies in a Networked Environment", Seminole, Fla. : Interpact Press, pp. 33 – 36
23. Uday S. Murthy, "An Analysis of the Effects of Continuous Monitoring Controls on e-commerce System Performance", *Journal of Information Systems*, Vol.18, No.2, Fall 2004.
24. VIRAN, M.; HAGA, W.J. (1999): "Password Security: An Empirical Study", *Journal of Management Information Systems*, vol.15, Iss.4, pp.161-185.

REQUEST FOR FEEDBACK

Dear Readers

At the very outset, International Journal of Research in Computer Application and Management (IJRCM) acknowledges & appreciates your efforts in showing interest in our present issue under your kind perusal.

I would like to request you to supply your critical comments and suggestions about the material published in this issue as well as on the journal as a whole, on our E-mail **infoijrcm@gmail.com** for further improvements in the interest of research.

If you have any queries please feel free to contact us on our E-mail infoijrcm@gmail.com.

I am sure that your feedback and deliberations would make future issues better – a result of our joint effort.

Looking forward an appropriate consideration.

With sincere regards

Thanking you profoundly

Academically yours

Sd/-

Co-ordinator

ABOUT THE JOURNAL

In this age of Commerce, Economics, Computer, I.T. & Management and cut throat competition, a group of intellectuals felt the need to have some platform, where young and budding managers and academicians could express their views and discuss the problems among their peers. This journal was conceived with this noble intention in view. This journal has been introduced to give an opportunity for expressing refined and innovative ideas in this field. It is our humble endeavour to provide a springboard to the upcoming specialists and give a chance to know about the latest in the sphere of research and knowledge. We have taken a small step and we hope that with the active co-operation of like-minded scholars, we shall be able to serve the society with our humble efforts.

Our Other Journals

