INTERNATIONAL JOURNAL OF RESEARCH IN COMMERCE, IT & MANAGEMENT

IJRCM

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-Gage, India [link of the same is duly available at Inflibnet of University Grants Commission (U.G.C.)],

Index Copernicus Publishers Panel, Polandwith 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 2401 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

CALL FOR MANUSCRIPTS

Weinvite unpublished novel, original, empirical and high quality research work pertaining to recent developments & practices in the area of Computer, Business, Finance, Marketing,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, Education, 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 mentionthe 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

FACTORS AFFECTING APPLICABILITY OF SECURITY CONTROLS IN COMPUTERIZED ACCOUNTING SYSTEMS

AMANKWA, ERIC
LECTURER
DEPARTMENT OF ICT
PRESBYTERIAN UNIVERSITY COLLEGE
GHANA

ABSTRACT

The challenges of security controls applicability in computerized accounting systems have been widely cited in the literature but research on the critical factors for preliminary and ongoing security controls application success is rare and fragmented. The purpose of this study therefore, is to investigate the critical factors affecting the application of security controls in Computerized Accounting Systems. The study also attempted to develop a framework for effective implementation of security controls in Computerized Accounting Systems throughout the system's lifecycle. Through a critical review of literature and empirical study using personal interviews, ten (10) factors were found to be critical for security controls applicability in computerized accounting systems - The study therefore found factors such as; Executive Support, Standardized IT Infrastructure, Experienced Project Manager, Security Awareness, Clear Security Objectives, Trained Human Resources, Organizational Culture, Total Cost of Ownership, Cryptographic mechanisms and User Involvement as critical. The Critical factors identified were classified into stages (chartering, project, shakedown, onward and upward) in Markus and Tanis' process-oriented model, to develop a comprehensive framework for practitioners and scholars.

KEYWORDS
Critical Factors, Applicability, Security Controls, Computerized Accounting, Information Systems.

INTRODUCTION

The importance of Security Controls in any computerized system cannot be overemphasized. A Security Control is a system that prevents, detects or corrects unlawful events in an organization. Security controls are needed in Computerized Accounting Information Systems (CAIS) to reduce losses (risks) by lowering likelihood of occurrence or by reducing the impact after a risk has occurred.

Computerized Accounting Information System (CAIS) faces 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, 2005), since information assets constitute a significant proportion of an entity's market value (ITGI, 2001). A growing body of research had also indicated that the existence and adequacy of security controls to protect Computerized Accounting Information Systems (CAIS) is essential (Abu-Musa, 2006) for the assurance of confidentiality, integrity and continuous availability of vital information for business continuity. COBIT's 2005 framework and Hicks (1999) have also touted security controls as indispensable to ensure more timely, accurate, relevant and reliable information from IT systems. Microsoft Corporation (2006), Flowerday & Rossouw (2005) and Amankwa (2012) have also stated that controls are also needed in Information Systems to prevent, detect and correct unlawful events with the capability of reducing the accuracy and reliability of information.

LITERATURE REVIEW

SECURITY CONTROLS OF COMPUTERIZED ACCOUNTING INFORMATION SYSTEMS

According to Laudon & Laudon (2010), IS Controls can be manual and automated, and consists of both general and application controls. 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.

Proper implementation of the selected security controls for an information system is very important, which can have major implications on the operations and a ssets of an organizationSecurity controls are the management, operational, and technical safeguards or countermeasures prescribed for an information system t o protect the confidentiality, integrity, and availability of the system and its information. A growing body of research indicates that the existence and adequacy of security controls to protect Computerized Accounting Information System (CAIS) 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.

The CEO and the CFO are required by Section 302 of the Sarbanes-Oxley Act to certify that financial statements fairly present the results of the company's activities and also require them to certify that they have evaluated the effectiveness of the organization's internal controls. Security control 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.

In a theoretical study conducted by Buttross and Ackers (1990), microcomputer security exposure and microcomputer organizational, hardware, software and data security controls were discussed. Their study provided security controls checklist that could be used to help the internal auditors in evaluating computer security.

In any current review Henry's (1997) contribution cannot be overlooked. Henry (1997) surveyed 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 form 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. Core characteristics of user-generated passwords and the associations among those characteristics were investigated in the study.

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. 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, agreed upon these top twenty critical security controls. The NSA, US Cert, the Department of Energy Nuclear Laboratories, DoD JTF-GNO, Department of State, DoD Cyber Crime Center plus the top commercial forensics experts and pen testers that serve the banking and critical infrastructure communities were all members of the Consortium. 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

CRITICAL SUCCESS FACTORS

These are factor whose failure could cause the computerized accounting systems and it security controls implemented to fail. A number or researchers have carried out various studies on the critical success factors for Information Systems, Security controls and Accounting Systems implementation. Those studies with direct correlation to the current study are considered in the selection of critical factors which are verified and validated in the empirical study. Selected studies and their selected critical factors are summarized in table 1 below. These factors shown in table 1 have been selected based on their frequencies of occurrence in previous studies. Only those factors which appear at least two times in previous studies have been selected to be empirically tested in the current study.

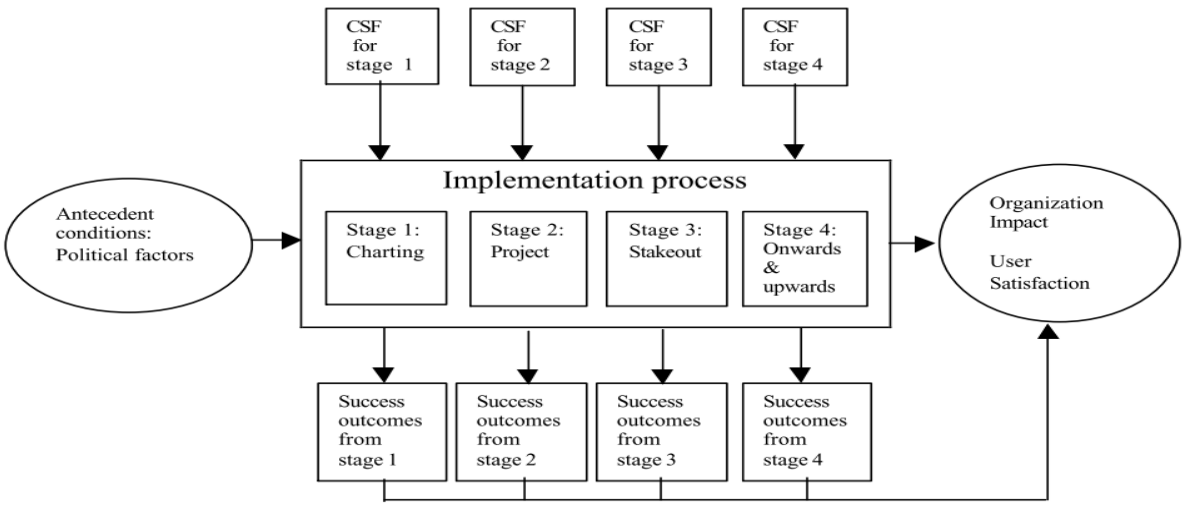
INFORMATION SYSTEM (IS) IMPLEMENTATION MODELS

To categorized the identified factors into stages in the IS life cycle to ensure successful applicability, two success-oriented model were found useful for achieving this goal. The six-phase model developed by Cooper and Zmud (1990) which consists of initiation, adoption, adaptation, acceptance, routinization, and infusion was the first to be considered. This model provides insight on the whole dynamic process of IT innovation. It was however realized that, the lines between the stages are hard for identification by practitioners, after a critical examination of the model. This limitation was however addressed by the four-stage model of Markus and Tanis (2000). The model focuses on the sequence of events leading up to implementation completion and identified the following four phases in an information System'slife cycle:

(1) Chartering: comprises decisions leading to the funding of a system
(2) Project: comprises activities intended to get the system up and running in one or more organizational units,
(3) Shakedown: stabilizing, eliminating ``bugs'', and getting to normal operations;
(4) Onward and upward: which continues from normal operation until the system is replaced with an upgrade or a different system.

This four-stage model was adopted for categorizing factors identified for two main reasons. First, it is deemed more comprehensible from a practitioner's perspective; second, existence of stage dependent success indicators in addition to the overall success (see fig 1) will help provide greater insight for conducting the study.

FIG. 1: RESEARCH MODEL (Markus & Tanis, 2000)



The chartering phase comprises decisions leading to funding of the CAIS project. Key players in the phase include vendors, Security consultants, company executives, and IT specialists. Key activities include initiation of ideas to implement CAIS, developing business case, decision on whether to proceed with Security Controls application or not, initiation of search for project leader/champion, selection of security controls and consultants, and project planning and scheduling.

The project phase comprises system configuration and rollout. Key players include the project manager, project team members (mainly from business units and functional areas), internal IT specialists, vendors, and Security consultants (implementation partners). Key activities include software configuration, system integration, testing, data conversion, training, and rollout. In this phase, the implementation partners must not only be knowledgeable in their area of focus, but they must also work closely and well together to achieve the organizational goal of security controls application in CAIS.

The shakedown phase refers to the period of time from ``going live'' until ``normal operation'' or ``routine use'' has been achieved. Key activities include bug fixing and rework, system performance tuning, retraining, and staffing up to handle temporary inefficiencies. In this phase, the errors of prior causes can be felt, typically in the form of reduced productivity or business disruption (Markus and Tanis, 2000). Hence, it is important to monitor and constantly make adjustments to the system until the ``bugs'' are eliminated and the system is stabilized.

The onward and upward phase refers to ongoing maintenance and enhancement of the new CAIS and relevant business processes to fit the evolving business needs of the organization. It continues from normal operation until the system is replaced with an upgrade or a different system. Key players include system developer, end users, and IT support personnel (internal and external). Security consultants may also be needed when upgrades are concerned. Key activities include continuous business improvement, additional user skill building, upgrading to new software releases, and post-implementation benefit assessment.

The phases in Markus and Tanis' (2000) IS life cycle model are in line with the stages of the traditional systems development life cycle, as presented in Figure1. As different factors are important in different stages, it is important to classify the factors identified into the phases of IS implementation life cycle where the factors may come into play (*see Figure 2*). Figure 2 shows the classification of these factors into an integrative framework

IMPORTANCE OF THE STUDY

From a practical standpoint, I.S developers, security consultants, Auditors, IT users and practitioners alike stand to gain from the findings of this study. The findings could therefore be used as a fundamental framework for implementing security controls in any computerized system. While there have been several studies on critical factors for information systems implementation, and a few on security controls implementation, none of the existing studies focused on critical factors for security controls implementation in computerized accounting systems. In view of this, this study bridges the existing research gap in Accounting and information Technology. It is also imperative to note that, the researcher at the time of this research was also unaware of any studies that investigated the critical factors affecting the applicability of security controls in computerized accounting system, hence the findings from this study provides valuable insights for top management CIO, and IT managers, to better understand non-technical issues in the systems lifecycle.

OBJECTIVES

Despite the vast benefits promised by Security Controls, it is however imperative to realize that these benefits can be realised through the successful application of Security Controls in Computerized Systems which is also highly dependent on a number of factors. This paper therefore investigates and discusses those factors critical to the successful implementation of Security Controls in Computerized Accounting Systems. Factors identified are also categorized using Markus and Tanis (2000) model into stages of the systems lifecycle, forming a comprehensive framework for security controls applicability in computerized accounting systems.

STATEMENT OF PROBLEM

In view of the problems above, the study attempts to; (1) investigate factors critical to the successful implementation of Security Controls in Computerized Accounting Systems and (2) proposes a framework for categorizing factors identified into stages of the systems lifecycle.

RESEARCH METHODOLOGY

The research method adopted in this study is a qualitative approach. This is because the research question requires an in-depth study into the processes of applying security controls in computerized accounting information systems. In addition, qualitative research is applicable to this exploratory novel study with a paucity of published research in the area. It also allowed the researcher to observe and understand the context within which decisions and actions regarding security controls applicability take place.

The primary data collection approach used in this research is interview which allowed the researcher to gather rich data from relevant Actors involved in various roles around the application of security controls. Interviews also helped to verify and validate the findings in the literature. The primary data used in this study was collected from the Presbyterian University College Ghana; a private University with well-equipped accounting offices in its four campuses, headed by the college's finance director. A total of five face-to-face semi-structured interviews were performed with the identified relevant Actors in the Security Controls application process. The identified relevant Actors included the College Accountant, Finance Director, Internal Auditor, Registrar, President, and System Administrator.

The secondary data on the other hand was collected through a critical literature review process. This allowed the author to identify primary studies that can be used to investigate a specific research question (Khan et. al. 2010) Through the critical literature review, ten articles that provide answers to the question: what are the key critical factors for Security Controls application success?, were selected. These ten articles were identified through a computer search of online databases of published works and conference proceedings in the information systems area. The articles were searched by the title based on the following criteria:

(1) "Critical success factors'' + "Information System Implementation"
(2)" Critical success factors" + "Security Controls"
(3) "Critical factors" + " Accounting Systems implementation" + "models"

In the case where the authors had published more than one article in the area, only the latest publication was used. Among the ten articles identified, US GAO (1999) was the earliest published work, whereas the other nine articles were published between 2000 and 2012. Table 1 summarizes the results of the review.

TABLE 1: SURVEY OF FACTOR AFFECTING APPLICABILITY OF SECURITY CONTROLS

	FACTORS AFFECTING APPLICABILITY OF SECURITY CONTROLS IN CAIS							
Studies/Authors	**Executive Support**	**IT Infrastructure**	**Project Manager**	**Trained HR**	**Security Aware-ness**	**Organi-zational Culture**	**ClearSecurity Objectives**	**User Involvement**
Nah & Lau (2001)	*		*	*		*		
Alshbiel & Al-Awaqleh (2011)	*	*		*		*		
Al-Awadi & Renaud (2008)	*			*	*		*	
Stahl & Pease (2007)	*			*	*		*	
Intan et. al. (2012)	*			*	*	*	*	
Ngai et. al. (2004)	*	*		*				*
US GAO (1999)	*		*		*		*	*
Extreme CHAOS (2001)	*	*	*				*	*
Li et. al. (2003)	*	*	*	*			*	*
Sanchez et. al. 2005	*		*	*		*		

From the review (table 1), eight factors emerged as critical to the successful applicability of Security Controls in Computerized Accounting systems. These eight factors were obtained after careful analysis and grouping of related sub-factors. These eight factors are inclusive of all the sub-factors identified in the review. These factors identified from existing literature and those from the empirical study conducted at the PUCG, were then categorized into the respective phases (shown in figure 2) in the Information System life cycle model proposed by Markus and Tanis (2000). A discussion of the importance of these factors in the application of security controls in computerized accounting systems was made.

This method seem to be the most appropriate for this study as it allows integration of ideas and experiences from both practitioners and scholars point of view. Practitioners, through the school of hard knocks and years of experiential analysis, have learned "what" seems to work and what doesn't. Scholars, through years of academic study and research, can tell us "why." By joining together the "whats and the whys", and throwing in a bit of 'common sense', the guidelines for successful application of Security Controls in CAIS can be strengthened. The approach parallels that of Nah and Lau (2001) and a very recent study by Iqbal et. al. (2012).

FINDINGS/RESULTS AND DISCUSSIONS

This study sets out with the aim of *investigating factors critical to the successful implementation of Security Controls in Computerized Accounting Systems*, using the Presbyterian University College Ghana (PUCG) as a case study. A careful analysis performed on the Security-Enhanced Computerized Accounting System developed and implemented at the PUCG, showed that the selection and implementation of effective security controls in any computerized system is not adequate to ensure a successful implementation throughout the system's lifespan. This is because; security controls are only a part of the larger system, and would need the other parts to be as effective as itself to achieve success. Just as the human system is made up of subsystems, with each performing a unique role to ensure a complete functioning human system; a computerized system is also decomposed into various sub systems. A system is defined as a set of inter-related components working within an environment to fulfil some purpose (Schwalbe, 2007). A computerized Accounting system therefore is an information system composed of hardware, software, policies (security controls), networks and people. These components must all be effective in order to achieve an effective and efficient system. If security controls are effective and working perfectly but other components such as hardware (Infrastructure), networks, software (OS) and people (Human Resource) are not effective, an efficient and successful implementation of the system cannot be realised. In other words, all components (subsystems) of the information system must be effective to ensure a successful implementation of a Security Control Computerized Accounting system.

The study therefore found factors such as; *Executive Support, Standardized IT Infrastructure, Experienced Project Manager, Security Awareness, Clear Security Objectives, Trained Human Resources, Organizational Culture, Total Cost of Ownership, Cryptographic mechanisms and User Involvement* as critical and essential for the successful implementation of security controls in any computerized accounting system. These factors are categorized into stages (Chartering phase, Project phase, Shakedown phase, onward and upward phase) of the Information Systems lifecycle using Markus and Tanis (2000) process oriented model as shown in figure 2 below.

EXECUTIVE SUPPORT

Executive support is needed throughout the implementation. The new system must receive approval from top management (Bingi, 1999; Buckhout, 1999; Sumner, 1999) and align with strategic business goals (Sumner, 1999). This can be achieved by tying management bonuses to project success (Wee, 2000). Top management needs to publicly and explicitly identify the project as a top priority (Wee, 2000). Senior management must be committed with its own involvement and willingness to allocate valuable resources to the implementation effort (Holland et al., 1999). This involves providing the needed people for the implementation and giving appropriate amount of time to get the job done (Roberts and Barrar, 1992).

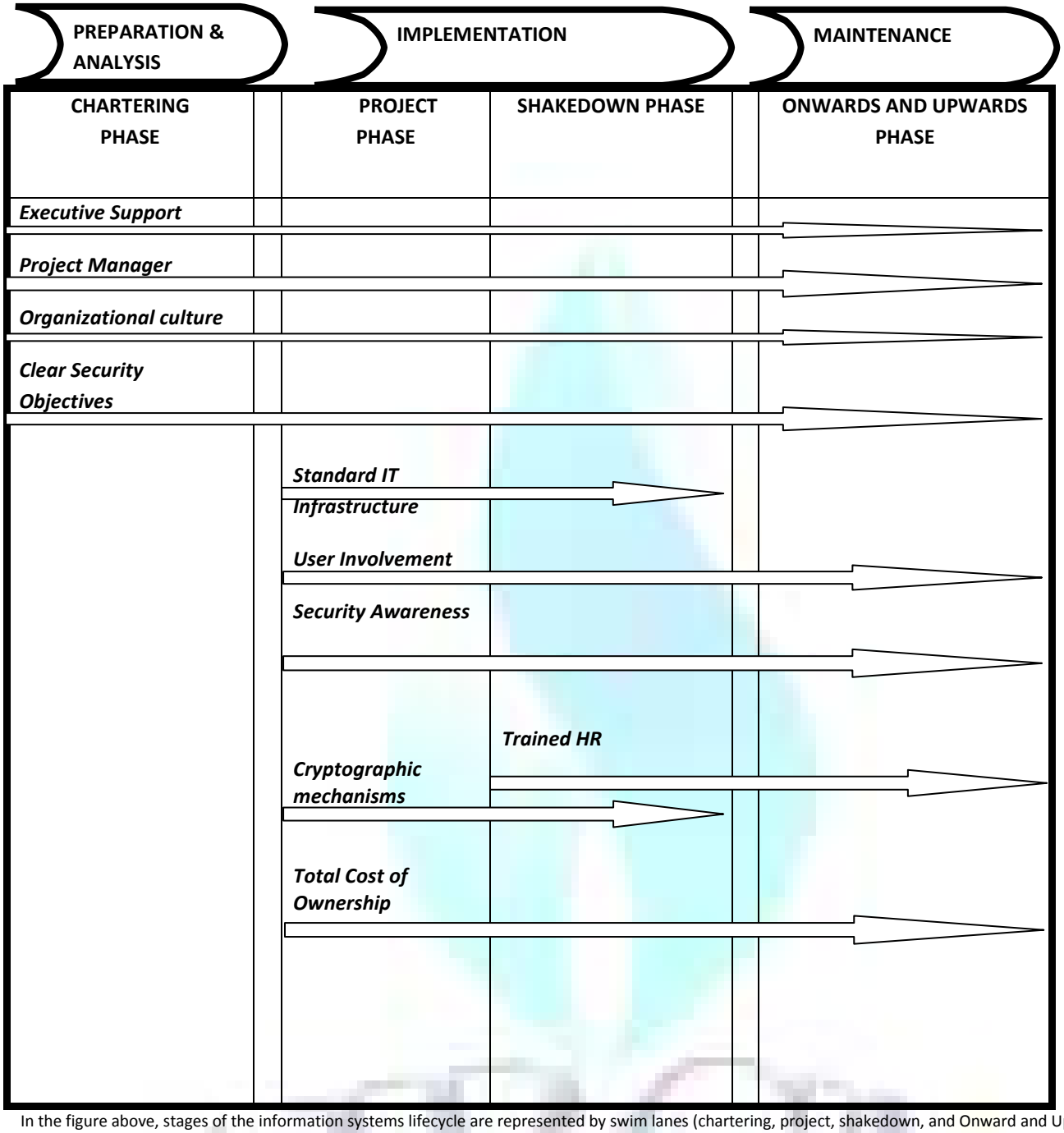
From the empirical study, it was realised that top management support is vital in all stages of the information system lifecycle. It was realised that IT support staff and security consultants could not accomplish projects without enough budget, in the shakeout stage, human resource training and policy support were necessary besides sufficient budget. In the onwards and upwards stage, the top managers should keep on supporting the project, in terms of taking feedback from key-users seriously, and maintaining and upgrading the system accordingly. This sentiment was reflected by several key IT support staff and was captured in the following quote: "…*with no attention from top managers, we could do nothing but watch the system fail in the fast changing internal and external environments*…" It was also realised that, the implementation of controls such as access control, segregation of duties, and other controls which puts some restrictions on users would require some backing from top management. In the empirical study conducted through interview, users emphasized their dislike for restrictions brought about as a result of the implementation of the security controls in the system. In view of this, if management do not show their total support for the success of the new system and it is left in the hands of these users to decide, the possibility of failure may be high. Hone & Eloff (2002) explain that the behaviour and attitudes of employees towards information security will be more in line with 'secure behaviour' if top management demonstrates concern. This therefore suggests that the tone of security is set by top management within the organization (Hinde 1998) and this would be achieved if security controls supports organizations core business functions (Blake, 2000). Executive support reflects the factors that influence managers to put commitment in security controls implementation and how employees respond to the need for having a high quality security system in the Computerized Accounting System. This relates to their actions on the ease of use and usefulness of the security system in protecting their financial information. When they support, they would change their perceptions regarding the benefits of adopting good security system (Lippert and Govindarajulu, 2006). During the empirical study, it was realized that, executive support is needed throughout the system's lifecycle. That is, all those activities leading to implementation in the Chartering phase of the model shown in figure 2, activities during implementation (Project and Shake down phases), and activities in final (Maintenance) stage of the system's lifecycle (that is onward and upward phase) should all be supported by top management to ensure successful applicability of security controls. In other words, the support of management is needed throughout the system's implementation.

ORGANIZATIONAL CULTURE

Organizational culture defined by Schein (1992) as "a pattern of shared basic assumptions that the group learned as it solved its problems of external adaptation and internal integration, that has worked well enough to be considered valid and, therefore, to be taught to new members as the correct way to perceive, think, and feel in relation to those problems". A culture with shared values and common aims is conducive to success. An emphasis on quality, a strong computing ability, and a strong willingness to accept new technology would aid in implementation efforts. Management should also have a strong commitment to use the system for achieving business aims (Roberts and Barrar, 1992). Users must be trained, and concerns must be addressed through regular communication, working with change agents, leveraging corporate culture and identifying job aids for different users (Rosario,2000). Many experts believe the underlying causes of many companies' problems are not the structure or staff, but the culture. According to Schwalbe (2007), Project work is most successful in an organizational culture where member identity, Group emphasis, Unit integration, Risk tolerance, Reward criteria, Conflict tolerance and Open-systems focus are highly prevalent. Encouraging a positive attitude throughout the organization towards the implementation of the new system is an important factor which can determine the success or failure of the system. in an organization where there is a positive culture towards information systems project, security controls applicability in computerized accounting systems is likely to receive the same positive attitude. However, where there is a negative attitude the new system may suffer. Top management must therefore encourage at all levels of the organization and inculcate in employees a positive security mindset before and during introduction of the system.

This culture of security consciousness must be present throughout the lifecycle of the system to ensure successful implementation. During analysis and preparation stage of the security controls application, management must insist and ensure a culture of security controls readiness by involving user of the system in the preparation work. This culture must be encourages during implementation (project and shakedown phase) and after implementation (onward and upward phase) to ensure success.

FIGURE 2: CLASSIFICATION OF CRITICAL FACTORS INTO MARKUS AND TANIS IS LIFECYCLE MODEL



In the figure above, stages of the information systems lifecycle are represented by swim lanes (chartering, project, shakedown, and Onward and Upward phases) and factors are classified under these stages. Block arrows depict the stages that the identified factors fall.

USER INVOLVEMENT

User involvement was identified as a key factor to the successful implementation of any Information System. Lack of user involvement traditionally has been the number one reason for project failure and conversely, the number one contributor to project success (CHAOS, 2001). No single quality of management practice is more highly correlated with success than employee participation. The question then becomes how to structure this participation to best ensure its success for the employee, the project and the organization. Baronas and Louis (1988) in their study to examine the effect change, propose that user acceptance of a new system would be facilitated when changes are realistically anticipated through input from knowledgeable sources; contrasts are given free expression through discussion among co-workers and between implementers and users; surprises are minimized through preview and realistic testing; and assistance is provided in coping through the availability and coaching of experienced implementers. System implementations often impose a threat of reduced control over a user's work. Baronas and Louis (1988) suggest that when employees are given the opportunity to enhance perceived control during a system implementation, they will adapt to the resultant changes and more readily accept the system. In addition, if an individual believes that the system is personally relevant, he will be more likely to form a positive attitude toward the system since attitudes are generally formed on the basis of beliefs. The strength of an individual's involvement is directly related to the extremity of his or her attitude toward the system. A high level of involvement could drive an extremely positive attitude. A low level of involvement, however, leaves a person susceptible to other influencers (e.g., persuasive forces, factual arguments). With increased user involvement and a positive attitude, users will have an increased desire to participate in implementation. Users sentiments on involvement are captured in the following quotation: "*we feel that we are a part of the system when involved and would do everything possible to ensure it succeeds. Contrary we feel management want to impose the new system on us and would abandon it with the least problem that occurs*" In the empirical study, it was realised that each user unit is a stakeholder and must therefore be considered. However, whether to actively involve these units in the process, who to involve and when, and how to involve them are the questions that remain unanswered. This is mainly because, choosing who to be involved requires building a team that can accomplish the tasks required of

them. It also requires building a team that will effectively represent the organizational issues that are being addressed by the project and will continue to support and integrate the new programs and processes into the post-implementation culture.

TRAINED HUMAN RESOURCE

Training and education are important for the successful implementation of any new system (Sprague and McNurlin 1993). Human resource is a term used to describe the individuals who make up the workforce of an organization. Dhillon (1999) argues that, organizations must have ongoing education and training programs to achieve the required outcome from the implementation of an information security policy. The efficiency and effectiveness of the system rely heavily on human resources since people are needed at all levels to operate, manage and use the Security Enhanced-Computerized Accounting System. Therefore users must have the requisite skills and experience, which is the main axis on which the computerized accounting system will succeed or fail. Ngai et. al (2004) argued that adequate training of the employees in an organization is important in allowing the benefits and advantages of using the Internet in SCM to be fully realized. Human resource is required to fill multiple functions in each of the departments of accounting and Information Technology within the organization. Stephen (1989) explained that the scientific and practical qualifications, experiences, technical skills and training are the most important specifications that must be available in the staff to achieve success. Al-Taweel (2001) also pointed out that, there is a lack of efficiency in the accountants, in the fields of using accounting systems. Therefore, to ensure success, Accountants and Accounting professionals who use and interact with the Security Enhance Accounting System must be equipped with the requisite technical skills. This was evident in the empirical studies through interview, as most users emphasized the need for periodic training in order to enhance their computing efficacy to resolve challenges from the system in a timely manner. This sentiment was expressed by several users of the system and summarized in the following quote "Since *the new system with security controls may come with new features, it will be prudent to organize training for staff periodically so that challenges with the new system could be addressed. When we encounter challenges which we are unable to resolve for a long time, we would have no other choice than to abandon the system"* Training, re-skilling and professional development of the IT workforce is critical. User training should be emphasized, with heavy investment in training and reskilling of developers in software design and methodology (Sumner, 1999). Employees need training to understand how the system will change business processes. There should be extra training and on-site support for staff as well as managers during implementation.

EXPERIENCED PROJECT MANAGER

An experienced project manager is essential for the successful implementation of IT projects (Schwalbe, 2007). Ninety-seven (97%) percent of successful projects had an experienced project manager at the helm of affairs (CHAOS, 2001). An individual or group of people should be given responsibility to drive success in project management (Rosario, 2000). First, scope should be established (Rosario, 2000; Holland et al., 1999) and controlled (Rosario, 2000). The scope must be clearly defined (Schwalbe, 2007) and be limited. This includes the amount of the systems implemented, involvement of business units, and amount of business process reengineering needed. Any proposed changes should be evaluated against business benefits and, as far as possible, implemented at a later phase (Sumner, 1999; Wee, 2000). Additionally, scope expansion requests need to be assessed in terms of the additional time and cost of proposed changes (Sumner, 1999). Then the project must be formally defined in terms of its milestones (Holland et al., 1999). The critical paths of the project should be determined. Timeliness of project and the forcing of timely decisions should be managed (Rosario, 2000). Deadlines should be met to help stay within the schedule and budget and to maintain credibility (Wee, 2000). Each of these activities must be lead by an experienced project manager who can provide direction and guidance for the success of the Information System project. Project manager's commitment is critical to drive consensus and to oversee the entire life cycle of implementation (Rosario, 2000). The project manager should also be in charge and should lead the project throughout the organization (Sumner, 1999), as transformational leadership is critical to project success. In any project, the project manager serves as the leader by providing directions for initiating, planning, executing, monitoring and controlling, and closing each phase of the project. In view of this, the project manager's expertise would be needed throughout the information system implementation cycle. People who conceive business ideas must be present and part of the team to develop plans for reaching set goal. In the same vein, those who plan must be part of the team to execute, in order to ensure proper interpretations of the plans. The project manager's experience from other projects would also be brought to bear, to ensure effective monitoring and controlling of project activities to achieve success. Therefore, an experienced project manager is needed in all stages of the system lifecycle as shown in figure 2 above.

CLEAR SECURITY OBJECTIVES

Security objectives must be clear enough and available at all levels of the organization for the perusal of all employees and must be aligned with the overall organizational security policy. A successful security journey, like a successful Information System project, requires many things, but one thing is definitely required: the knowledge of your destination. On any project, being able to articulate the business objectives is key to success. A project without a stated destination will likely go in many directions, none of them resulting in the desired effect. Without clearly articulated and understood security objectives, not only will the road to successful implementation be bumpy, but you won't know when the desired outcome is realized because you don't know what exactly what the implemented security control is to achieve. Clear objectives help project teams prioritize their focus on performing the work that best achieves the objectives. A shared vision of the organization and the role of the new system and structures should be communicated to employees. There should be a clear business model of how the organization should operate behind the implementation effort (Holland et al., 1999). There should be a justification for the investment based on a problem and the change tied directly to the direction of the company (Falkowski et. al., 1998). Security mission should be related to business needs and should be clearly stated (Roberts and Barrar, 1992). Goals and benefits should be identified and tracked (Holland et al., 1999).

It is imperative to ensure that, all involved in the analysis and preparation (Chartering phase) work for implementation, have a clear understanding of the set security objectives to be realized from the implementation to avoid any deviations. If security objectives are clear, plans would be geared towards achieving the set goals. However, if security objectives are ambiguous and are subject to several interpretations, they would be interpreted differently by different individual. Clear security objective are required throughout the implementation processes (that is from chartering, through to project and shakedown and finally onward and upward).

SECURITY AWARENESS

The interviews and existing literature showed that, organizations all wished to secure their information. However, they believed that information security would be achieved simply by increasing security awareness and providing training. All experts stressed the need for periodic security awareness programmes for employees. One of the experts commented: " *Years ago security awareness was zero, a lot of people thought that all they needed to be protected was to have login name and password, so we worked on training our employees to raise the awareness and this made the implementation of security controls easier*". Furthermore they stressed that information security would need a continuous and ongoing awareness and training programme for employees to deal with the ever-changing security arena. A citation by McKay (2003) on the 2002 security awareness index report indicated that organizations around the world are failing to make their employees aware of the security issues and the consequences thereof. However, there is no evidence in the literature that awareness programs play any decisive role in reducing insecure behaviour or that it makes a difference in ensuring information security and in increasing compliance to information security policies. Notwithstanding this, making employees aware of the rationale behind the introduction of security controls, create a common understanding and cordial working relationship between employees and management. This makes both parties relaxed and more comfortable in the discharge of the duties within the organization. Top management expressed in the empirical study that "*we are now more comfortable and can trust information generated from the computerized accounting system for decision*". Employees on the other hand indicated that "*since we know what security controls exist and what they are to achieve, we are more relaxed when working the system*". On the part of employees, realizing the different security features introduced in the new computerized accounting system (for example, access controls, multifactor authentication, and internal audit log for ensuring non-repudiation) boosted their confidence when

working with the system. An employee indicated that, now that there is an internal audit log to monitor who did what; cases of people being accused wrongly will now be a thing of the past.

STANDARDIZED IT INFRASTRUCTURE

Information technology standardization is a strategy for minimizing IT costs within an organization by keeping hardware and software as consistent as possible and reducing the number of tools you have that address the same basic need. The successful implementation of a Security Enhanced Computerized Accounting Information System is not only dependent on the adequacy of selected controls but also on the existence of standardized IT infrastructure. Standardizing IT infrastructure has benefit of minimizing IT cost and hence the total cost of implementing the computerized system. It may take the form of ensuring that every computer has the same operating system, or of purchasing hardware in bulk so that every PC in the office is the same make and model. The standardized infrastructure and platform introduces controls through the use of standards and policies to manage desktops and servers, how machines are introduced to the network, and the use of Active Directory directory services to manage resources, security policies, and access control. Customers in a standardized state have realized the value of basic standards and some policies, yet they are still quite reactive.

From the empirical study, it was realized that, if the IT infrastructure is not standardized, what work perfectly on one part of the network would would not work on other parts. When different Operating Systems are used on computers within the network; implementing security controls becomes a daunting task, as different levels of controls would have to be implemented on the different operating systems to surmount compatibility issues. Also different versions of the security-controls enhanced computerized accounting information system would have to be developed. For instance, in an organization that uses both Windows and Linus operating systems, any information system (I.S) developed must take cognisance of this dynamics. This simply would require the development of two different versions of the same I.S, and thereby increase cost. In organizations where IT infrastructure is standardized, implementing security policies is much easier, as a single policy can be replicated in all parts of the organization without any difficulty. The lack of standardized IT infrastructure leads to inconsistent support for end user. Incidents, requests, and problems therefore become difficult to track and deal with. Standardization IT infrastructure therefore enhances user needs and user experience in order to increase productivity and amplify the impact of employees.

TOTAL COST OF OWNERSHIP

Factors which were not present in the literature from existing empirical studies also emerged, and one of such factors is total cost of ownership (TCO). Total cost of ownership (TCO) is a financial estimate whose purpose is to help consumers and enterprise managers determine direct and indirect costs of a product or system. TCO (total cost of ownership) is recognized as the industry-standard method for the financial analysis of IT and other enterprise costs. In the face of tighter financial controls and increasingly expanding IT influence, TCO analysis is more important than ever. It's been adopted by industry-leading IT providers, users and industry analysts (Mieritz, and Kirwin, 2005). According to Mieritz, and Kirwin, (2005), "Ownership" expresses the asset-based philosophy and that all costs in TCO are embedded in "IT assets," which include IT and the people using it, all of which are owned by the enterprise. For example, TCO can be expressed as the total cost of a Windows PC, a Unix server, a structured task worker or a knowledge worker.

In the empirical studies conducted through personal interviews, it was realised that total cost of ownership is deemed an important factor to the successful implementation of an information system from both management and users perspectives. Management emphasized in the interview that if cost brought about as a result of the implementation of the new system is on the high side and is not a one-time cost, but persistently puts pressure on the organizations budget, then the organization would be forced to consider other options, irrespective of the advantages promised by the new system. User in the accounts and IT departments also shared the same view in different words by stressing that if management is unable to meet the financial requirements imposed on the organization by the new system in a timely manner, it would impact negatively on productivity, which could lead to eventual abandonment of the system.

CRYPTOGRAPHIC MECHANISM

Cryptography is the study of how to obscure what you write so as to render it unintelligible to those who should not read it. Cryptography is used to transform usable accounting information into a form that renders it unusable by anyone other than an authorized user. Cryptography helps to protect the integrity and confidentiality of information transmitted over networks. The most frequently applied Cryptographic schemes are; Encryption algorithms, Digital signatures and Cryptographic hash functions (Gollman, 2006).

One important factor which came out during interviews with security consultants and IT staff was the choice of cryptographic mechanisms for assuring information confidentiality, integrity and availability (CIA). They argued that if the right cryptographic mechanisms are not used to ensure proper protection of vital organizational assets (information), the system would not be reliable for decision making; information will not be complete and available in a timely manner. When this goes on over a period of time, the system may lose its 'value' and the organization will be forced to phase it out.

CONCLUSIONS AND RECOMMENDATIONS

This paper puts forward the critical success factors for security controls implementation in computerized accounting information systems (CAIS). Findings generated from existing literature and empirical studies using the Presbyterian University College Ghana (PUCG), the findings can be used as the basis for security controls implementation in other computerized systems. A total of 10 critical success factors for Security Controls implementation in CAIS have been identified, based on a review of literature and empirical studies at the PUCG. The study provides an insight into how security controls can be successfully implemented in computerized systems. The critical success factors identified in the IS implementation process offer interested practitioners a better understanding and facilitate them in adjusting their business strategies accordingly. Finally, the study categorized the critical success factors into stages in the systems lifecycle, serving as a fundamental framework for both practitioners and scholars.

SCOPE FOR FURTHER RESEARCH

This study provides a theoretical framework for security applicability in computerized accounting systems with no empirical proofs, therefore further research could be carried out to test the framework empirically for additions and subtractions of the factors identified.

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 Al-Awadi M. and Renaud K. (2008): "Success Factors In Information Security Implementation In Organizations", Information Resources Management Journal, Vol. 18

3 ALshbiel Seif Obeid and Al-Awaqleh Qasim Ahmad (2011): "Factors Affecting the Applicability of the Computerized Accounting System, Jordanian Ministry of Health (Field Study on Governmental Hospitals in the North Territory)", International Research Journal of Finance and Economics, EuroJournals Publishing, Inc, ISSN 1450-2887 Issue 64

4 Amankwa Eric (2012): " Assessment of Security Controls in computerized Accounting Information Systems – The case of Presbyterian University College", Lambert Academic Publishing – Saarbrucken Deutschland Germany, pp.22

5 Baronas Ann-Marie and Meryl Reis Louis, (1988) "Restoring A Sense of Control During Implementation: How User Involvement Leads to System Acceptance." MIS Quarterly, March, 1988, (12:1), pp. 111-123

6 Bingi, P., Sharma, M.K. and Godla, J. (1999), ``Critical issues affecting an ERP implementation'', Information Systems Manag

7 Black, S., 2000. Protecting the Network Neighbourhood. Security Management, Vol. 44, No. 4, pp. 65-71.

8 Buckhout, S., Frey, E. and Nemec, J. Jr (1999), ``Making ERP succeed: turning fear into promise,'' IEEE EngineeringManagementReview,pp. 1
9 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
10 Control Objective for Information and related Technology (COBIT), 4th Edition, (2005), COBIT FRAMEWORK 4.0, IT Governance Institute press, USA
11 Cooper, RB & Zmud, RW (1990), 'Information Technology Implementation Research: A Technology Diffusion Approach', Management Science, vol. 36, no. 2, pp.123-139.
12 Dhillon, G., 1999. Managing and Controlling Computer Misuse. Information Management & Computer Security, Vol. 7, No. 4, pp. 171-175.
13 Eduardo Frenandez-Medina and Marino Piattini, "Designing Secure Databases", Information and Software Technology Journal, Vol. 47, 2005.
14 Extreme CHAOS (2001), The Standish Group International Inc.
15 Falkowski, G., Pedigo, P., Smith, B. and Swanson, D. (1998), ``A recipe for ERP success'', Beyond Computing, pp. 44-5.
16 Fiona Fui-Hoon Nah and Janet Lee-Shang Lau (2001): "Critical factors for successful implementation of enterprise systems", Business Process Management Journal, Vol. 7 No. 3, 2001, pp. 285-296
17 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
18 Gollmann Dieter (2006), Computer Security-2nd Ed. John Wiley & sons Inc, England.
19 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.
20 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.
21 Hicks J.R (1999) Accounting Packages, Portsmouth Business School Press, p. 7-10
22 Hind, S. 2002. Security Surveys Spring Crop. Computers and Security, Vol. 21, No. 4, pp. 310-321.
23 Holland, P., Light, B. and Gibson, N. (1999), ``A critical success factors model for enterprise resource planning implementation'', Proceedings of the 7th European Conference on Information Systems,Vol1,pp.273-97.
24 Holland, P., Light, B. and Gibson, N. (1999), ``A critical success factors model for enterprise resource planning implementation'', Proceedings of the 7th European Conference on Information Systems,Vol1,pp.273-97.
25 Hone, K. & Eloff, J.H.P. 2002. What makes an Effective Information Security Policy. Network Security, Vol. 20, No. 6, pp. 14-16.
26 Intan Salwani Mohamed, Izzatul Husna, Dr Norzaidi Mohd Daud, Zakiah Baharin and Saidin Wan Ismail (2012): "Accessing Drivers for Organizational Commitment Towards the Security Controls Implementation in the Malaysian Online Service in Computer-Based Accounting System", Advances in Natural and Applied Sciences 6(8): 1223-1237
27 Iqbal U., E. Uppstrom, G. Juell-Skielse (2012): "Cloud ERP implementation challenges: A study based on ERP lifecycle model", Advances in Enterprise Information Systems II, Taylor & Francis Group, London
28 ITGI (IT Governance Institute). IT governance executive summary; board briefing on IT governance. Rolling Meadows, 2001.
29 José Luis Sánchez; Stefan Savin; Virginia Vasileva (2005): "Key Success Factors In Implementing Electronic Medical Records In University Hospital of Rennes", Europhamili / Aesculapius Professional Study, 2005 - ENSP Rennes, France
30 Laudon C. Kenneth and Laudon P. Jane (2010): " Management Information Systems, Managing the Digital firm, Eleventh edition", Pearson Education, Inc, Pp. 338
31 Li Huixian, Lim John, Raman K.S. (2003): "An Exploratory Case Study on IS Implementation and Organizational Change in China", Proceedings of the 11th European Conference on Information Systems, ECIS 2003, Naples, Italy
32 Lippert, S.K. and C. Govindarajulu, 2006. Technological, organizational, and environmental antecedents to web services adoption. Communications of the IIMA, 6(1): 146-158.
33 Markus, ML & Tanis, C (2000), 'The Enterprise Systems Experience - From Adoption to Success', in Framing the Domains of IT Management: Projecting the Future through the Past, ed. RW Zmud , Pinnaflex Publishing, Cincinnati, OH, pp.173-207.
34 McKay, J. 2003. Pitching the Policy: implementing IT Security Policy through Awareness. SANS Institute.
35 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]
36 Mieritz Lars and Kirwin Bill (2005): "Defining Gartner Total Cost of Ownership", Gartner Inc. ID Number: G00131837
37 Moscove, Stephen A., "E-Business Security and Controls", CPA Journal, Vol. 71, Issue 11, Nov2001.
38 Ngai, E. W. T., Cheng, T. C. E. and Ho, S. S. M. (2004), "Critical Success Factors of Web-based Supply Chain Management System Using Exploratory Factor Analysis", Production, Planning & Control, Vol. 5, No. 6, pp. 622 - 630.
39 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.
40 Roberts, H.J. and Barrar, P.R.N. (1992), ``MRPII implementation: key factors for success'', ComputerIntegratedManufacturing Systems,Vol. 5No. 1, pp. 31
41 Rosario, J.G. (2000), ``On the leading edge: critical success factors in ERP implementation projects'',BusinessWorld, Philippines.
42 SANS Cyber Defense (2010) 20 Critical Security Controls [Online] Available at: http://www.sans.org/critical-security-controls [Accessed on 5th November, 2010]
43 Schein EH. Organizational Culture and Leadership. Jossey-Bass, San Francisco. 1992.
44 Sprague, R. H. and Mcnurlin, B. C., 1993, Information Systems Management in Practice (New Jersey: Prentice Hall).
45 Stahl Stan, and Kimberly A. Pease (2007): "Effectively Managing Information Security Risk, A guide for executives", Citadel Information Group, Inc. Los Angeles. Pp. 8
46 Stephen A. Moscove, Mark J., Seemkin (1989), accounting information systems for decision-making concepts and applications-, the translation of Kamal El-Din Saad, Ahmed Hamed Hajjaj, AlMareikh Publishing House, Riyadh, Saudi Arabia, 1989, p. 802, p.803.
47 Sumner, M. (1999), ``Critical success factors in enterprise wide information management systems projects'', Proceedings of the Americas Conference on Information Systems (AMCIS), pp.232-4.
48 United States General Accounting Office (GAO) (1999): "Information Security Risk Assessment Practices of Leading Organizations, A Supplement to GAO's May 1998 Executive Guide on Information Security Management, GAO/AIMD-00-33
49 Wee, S. (2000), ``Juggling toward ERP success: keep key success factors high'', ERP News, February,available at: http://www.erpnews.com/erpnews/erp904/02get.htm

REQUEST FOR FEEDBACK

Dear Readers

At the very outset, International Journal of Research in Commerce, IT 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 i.e. **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