International Journal of Computer (IJC)
ISSN 2307-4523 (Print & Online)

http://ijcjournal.org/

A Framework for Improving Computer-based Information Systems Auditing

Yusuf Sheikh Khalif Abdirahman*

Jomo Kenyatta University of Agriculture and Technology, School of Computing and Information Technology
Hodan district, Mogadishu, Somalia
Email: kaariye2012@hotmail.com

Abstract

Although Enormous investment is currently being made in computer-based information systems but many of them suffer chronic problems of information security and efficiency [1]. There is a concern about whether the standard quality and security of computer-based information systems is being achieved. As a consequence, growing attention is being paid to evaluating the information systems [2]. The main purpose of this paper was to propose a framework for improving computer-based information systems auditing. The study has two main features; firstly it structures the audit process; secondly it allows the evaluation of computer-based information systems according to a specific set of criteria based on quality, security, compliance and readability requirements. A descriptive survey research design was conducted to gather the primary data. In this paper, the researcher identified shortcomings of some accredited existing IT audit frameworks, and proposed an improved model of audit framework that addresses the main aspect of information security and performance. Therefore, the main purpose of this paper is to come out with a holistic Information System Audit framework that incorporates the general aspects of other important IS audit frameworks that can serve as a guide in Information System Audit for large and medium-sized institutions.

Keywords: information system; information auditing; information security; information efficiency.

1. Introduction

As the organizations are becoming increasingly dependent upon information systems (IS) and information technology (IT), the importance of implementing information best practices, standards and methodologies, producing highly secure information and quality services is evident [3].

---

* Corresponding author.

The study was carried out to identify some of the major gabs in the information system Auditing approaches currently on the market and propose a new information auditing method called INFO-AUDITOR that can fill those gabs which can be used as information systems audit for both large and medium-sized institutions. In order to ensure that the information security and effectiveness requirements are addressed, this paper focused on suggesting a new information audit approach to secure and improve information system. The identified security challenges and ineffectiveness were mapped. Information systems and information technology audit frameworks try to evaluate the system's internal control design and effectiveness. Information systems and technology frameworks attempt to establish a process for evaluating efficiency and security protocols, development processes, and IT governance. Information system audits are used to evaluate the organization's ability to protect its information assets and to properly dispense information to authorized parties.

2. Materials and Methods

In order to ensure that the information security and effectiveness requirements are addressed, this paper focused on developing a framework to secure and improve information system. The information security and effectiveness challenges of the studied organizations were addressed. The identified security challenges and ineffectiveness were mapped. In this study hybrid approach was used. COBIT, and ISO 38500 frameworks were combined to come up with the required Framework. The two frameworks were found to have sufficient security controls and information effectiveness which complement each other. The paper has two main features; firstly it structures the audit process; secondly it allows the evaluation of computer-based information systems according to a specific set of criteria based on quality, security, compliance and readability requirements. A descriptive survey research design was conducted to gather the primary data. This paper discusses two frameworks for the information audit: Control Objectives for Information and Related Technology (COBIT), and information security standard published by the International Organization for Standardization (ISO). The purpose of this discussion was to identify the relationships between these frameworks and to propose extensions for a new model.

3. Results

To ensure that information systems are functioning in an efficient and effective manner and to help the organization achieve its strategic objectives, an audit process must be performed. This task involves analyzing information systems processes. Individual activities within an information system can be grouped into processes. The security and audit framework for information is essential for the information system and technology because it provides assessment and evaluation of the information security and quality [4]. The end result of this new paper will serve as an effective guidance in information system auditing.

A Set of criteria those related to business requirements for information considered by different information audit frameworks [4] are.

- Quality requirements of outputs encompassing for example efficiency and performance.
- Security requirements described by the criteria of consistency, security, conformity and reliability.

- Readability requirements comprising feasibility, auditability and ability to evolve.

The paper have used customized and hybrid approaches to come up with the new framework. The data gathered from primary and secondary sources has been used to develop the new framework. The researcher used the collected information from primary data to create a criterion to filter the findings. The summary of the findings mapped against COBIT and ISO frameworks are summarised in fig 1.

RESEARCH FINDINGS	**COBIT**	**ISO38500**	**PROPOSED FRAMEWORK**
There is lack of professional IT staff in telecommunication companies	Planning and Oganisation -Manage human Resource	Communications and Operations management - operational procedures and responsibilities	Plan and organize PO2
Information security is not given priority	Delivery and Support -Identify and allocate cost	--	Acquire and implement AI3
Employees Lack proper training.	Delivery and support - Educate and train users	Personnel security -User training	Acquire and implement po2
Laws are not adhered	Planning and organisation – Ensure compliance with external requirements	Compliance Management -Policies and procedures	Plan and organize PO4
user name and password leakage	Monitoring - Assess internal control adequacy	Access controls -User access management and user responsibilities	Assed and evaluate AE1
Hacking information systems	Monitoring - Assess internal control adequacy	Access controls - access control and monitoring system	Asses and evaluate AE3
Data stealing	-	System development and control of interactions between internal and third parties at information exchange and cryptographic controls	Plan and organize PO4
viruses and malicious Software attacks.	Monitor Security Posture - Monitor security Safeguards	Communications and Operations management - Protection against malicious software	Asses and evaluate AE1
Lack of Physical security	Delivery and support –manage facilities	physical and environmental security and procedures of physical hazards	Deliver and support DS5
Lack of authorization and authentication controls	Acquisition and Implementation - manage changes	Access controls -User access management and user responsibilities	Assess and Evaluate AE1
Firewall absence		Communications and	Assess and Evaluate

		operations -Network security management	AE1
Intrusion detectors are not used	Acquisition and Implementation - identify automated solutions	Communications and operations management --Network security management.	Assess and Evaluate AE3
Lack of Risk assessment	Planning and organisation - Assess risks	Business continuity management and disaster recovery plan	Assess and Evaluate AE4
Managers neglect information security.	Planning and organisation -Communicate management aim and direction	Personnel security -Responding to security incidents and malfunctions	Acquire and implement AI3
Data Transmission policy lacked	Planning and organisation -Manage IT investment	Communications and Operations management -Exchanges of information and software with other organisations	Acquire and implement AI3
portable devices are threat	-	Access control -Mobile computing and Teleworking	Plan and organize PO1
Ant viruses are not used	Acquisition and Implementation -acquire and maintain application software	- -	Plan and Organize PO1

Figure 1: mapping INFO_AUDITOR against COBIT and ISO

To ensure that information systems are functioning in an efficient and effective manner and to help the organization achieve its strategic objectives, an audit process must be performed [5]. This task involves analyzing information systems processes. Individual activities within an information system can be grouped into processes. The fundamental feature of this framework is that audit domains and audit criteria can be combined to form a hierarchical tree consisting domains, processes and activities.

The proposed framework has four domains resulted from grouping the related processes to improve information security and effectiveness in an organization.

The new framework named The INFO-AUDITOR identifies four domains and 21 processes. These domains are:

- Plan and organize
- Acquire and implement
- Deliver and support
- Assess and evaluate

Each domain has other primary processes, many of which are derived from other internationally recognized security and audit frameworks. A process is what has to happen to achieve information security and effectiveness objectives [6]. Each primary process has activities that give direction of how information efficiency will be implemented within a process.

quality	Conformity with user needs	
	User satisfaction	
	Objective achievements	
	Conformity with specification	
	Parallel procedure existence	
Compliance with laws	Condition compliance	
	Compliance with laws and Regulations	
	Compliance with International standards	
Effectiveness	Efficiency	
	Profitability	
	Performance	
security	Consistency	Access controls
		Security techniques control
		Application controls
		Result controls
		Anti intrusive tests
	Reliability	Data backup
		Business continuity plan
		Failure procedure
		Breakdown resistance
	Readability	Feasibility
		Auditabilty
		Ability to evolve
	Integrity	Norms and standards
		documentation

Figure 2: Real life example

4. Discussions

A key element of IS auditing is the alignment of business and IT in order to achieve the desired business goals. The achievement of this alignment requires the implementation of a suitable IS auditing framework for IT management. This paper surveyed and discussed audit approaches used in the information evaluation process. The paper defined a domain-based approach allowing auditors to perform in an effective and efficient way of information system audit process. This framework helps auditors, companies and users in structuring the audit process using relevant criteria. It proved to be a cost-saving approach in information audit practice. COBIT drawback is that it is a practitioner based approach. It is not theoretically based approach [7]. This approach can been used to audit several domains providing an alternative to COBIT. The main principles and practices of ISO and COBIT can be incorporated into the INFO_AUDIT framework. The analysis of this paper shows that this framework identifies threats and challenges faced by information systems and investigates the techniques and approaches used for auditing information and develops an audit framework to keep information efficient and protected. The fundamental feature of this framework is that audit domains and audit criteria can be

combined to form a hierarchical tree consisting domains, processes and activities. A fundamental drawback of this IS auditing framework is a lack of consideration of the interdependencies between criteria. Another major limitation is that the framework may face a problem in analytic hierarchy process for multi-criteria decision making. Finally the framework has not fully addressed evaluation measures in the cases of unexpected activities.

5. Recommendations

The recommendations of the study based on the findings:

- The study suggests that each organization should increase the funds allocated for information security and auditing.
- Information audit practices, measures and procedures should be applied.
- Information security measures and procedures should be adhered.
- Information technology staff with the necessary skills should be engaged and capacity building should be done regularly.

References

[1] N. Merson. “Information Technology Audit: Systems Alignment and Effectiveness Measures”, Ph.D Dissertation, AUT University, U.S.A, 2008.

[2] J. Akoka. “ A framework for auditing web-based information ” presented at the 18th European Conference on Information Systems, in proc. ECIS2010-0297, 2010, pp.11

[3] Thomas yeboah, (2013, Jul). “A Proposed Information Technology Audit Framework For Microfinance Kumasi ” Journal of Engineering, Computers & Applied Sciences (JEC&AS)[.online], vol. 2, pp 23, Aug, 2013.

[4] S. Nderitu. “A Framework to Extend COBIT Security Framework to Overcome Confidentiality Threats in Electronic Commerce”, M.S Dissertation, jkuat University, Kenya, 2015

[5] Anderson. J. (2009, Mar 15). Evaluation of information technology in the delivery of health care using computer simulation (1st edition). [On-line]. available: http://www.lewingroup.com [Jul 10, 2014]

[6] B. Peny(2012 Feb 12.) Product, project and programme evaluation (1st edition). [On-line] Available: http://www.lewingroup.com [march 15,2015].

[7] S.Wang.“Toward a General Model for Web-Based Information Systems”, International Web Site Audit and Evaluation”, http://www.lewingroup.com, Nov.26, 2010[2015].