ISSN: 4792 -61X2
Volume 8, Number 1, 2022
Innovative Journal of Marketing, Management and Accounting Research

INFORMATION SECURITY AUDITS AND ADMINISTRATIVE EFFECTIVENESS IN STATE-OWNED UNIVERSITIES IN RIVERS STATE

[1]Prof. Sam Otamiri and [2]Tariere Fortunate Nwibani
[1]Department of Office and Information Management
[2]MSc Student, Department of Office and Information Management
[1&2]Faculty of Management Sciences, Ignatius Ajuru University of Education
Rumuolumeni Port Harcourt, Rivers State, Nigeria

samotamiri@yahoo.com

ABSTRACT

Businesses have major goals that includes increase in profit, larger market share, counter competition and brand identity process. In order to achieve these goals, institutions must rely on constant flow of information. Hence, the need for implementation of information security audit. This study sought to determine the extent to which information security audit correlate with administrative effectiveness in state-owned universities in Rivers State. The study adopted a research survey design to assess the correlation between information security audits and administrative effectiveness in state-owned universities in Rivers State. The population for this study comprised of two hundred and ninety-sixty (296) administrative staff of the two state-owned universities in Rivers State. For this study, the researcher conducted census survey and as such there was no sample size drawn from the population. Census survey is a complete listing of all the items in the population. It is studying the entire population without drawing a sample size. The study used questionnaires to collect primary data from the respondents. Two sets of questionnaires used were titled Information security audits Questionnaire (ISAQ) and Administrative Effectiveness Questionnaire (AEQ). Reliability of the questionnaire was evaluated through Cronbach's Alpha test which measures the internal consistency. A reliability coefficient of 0.89 was obtained. Mean and Spearman ranked correlation was the means of analysis. The results revealed very weak to very strong positive relationship between Info-security audit and measures of administrative effectiveness. The study concluded that information security audit is very important for improving administrative effectiveness in the organizations. Based on the findings of the study and conclusions drawn, it was recommended that Management of the universities are highly encouraged to develop a clear strategy to allow for increased role of general controls of information security system in improvement of their problem solving and decision-making process.

Keywords: Information Audit, info-security, administrative effectiveness

INTRODUCTION

In the educational sector, especially in the state-owned universities, administration is perceived as activity done in order to plan, organize and successfully run a business, school or other institution. It is a process or act of organizing the way that something is done. Administration according to Eden (2016) involves planning activities which aim at the fulfilment of the goals of a particular organization or institution. It calls for the ability of the administrators to make the right decisions to fulfil the required goals. Therefore, in the educational setting, administration has been extended as a service activity or tool through which the fundamental objectives of the institutional process may be efficiently optimized when allocating human and material resources as well as to make the best use of existing resources.

Administrative personnel in the state-owned universities undertake duties in which they are allocated. They contribute to the aims and objectives of institutions. However, the issues faced by office administrators in their working life are different; most especially as many studies revealed the need for the integration of digital technology into administrative activities of state-owned universities. For example, an administrator in the tertiary institution may be obliged to deal with

issues such as "technology and economic challenges, decision making processes, etc (Tang & Chamberlain, 2017). In any given organization, to record an effective administration, it must adapt to have the capability to strive continuously in a dynamic business environment (Whitman et al, 2014). Chu (2015) contented that in the turbulent political, socio-cultural, economic and technological environment, institutions must be ready to experience disruptions in their day-to-day activities. For instance, an unprepared organization can be adversely affected by a change in the political environment. On the other hand, a well-prepared organization will benefit immensely from the change as a result of the information securities strategies already put in place. These challenges can manifest numerous threats to the business existence. Crises may suddenly happen from a number of sources, but regardless of their severity or intensity, the challenges need varying approaches to deal with them.

Businesses have major goals that includes increase in profit, larger market share, counter competition and brand identity process. In order to achieve these goals, institutions must rely on constant flow of information (Surcel & Amancei 2017). Within this context, it is deduced that information has become the lifeblood of modern institutions and is core to most business processes today, therefore necessitating optimal protection. As state-owned universities today deal more with electronic information, they have realized that information security issues need to be accorded great importance in line with other business requirements by focusing on four tactical areas including strategy and business alignment, organization and culture, management and governance, and, technology.

The educational sector, including state-owned universities, has witness a rapid rise in the number of electronic crimes that use pharming and smashing involving Internet browsers and mobile devices to steal personal and financial information and in some cases academic records falsification/alteration (Kim, 2013). Also, hike in the management of crises and disasters has become a major concern for both practitioners and academics. Natural disasters, pandemic disease, terrorist attacks, economic recession, equipment failure, cyber-crimes and human error can all pose both a potentially unpredictable and severe threat to the continuity of an organization's operation (Xiao & Cao, 2017). The annual number of these high-risk events worldwide has steadily increased and the direct loss increased by $ 250 billion from $ 50 billion (UN in Xiao & Cao 2017). With the recent increase in the number of new types of serious electronic frauds, the importance of information security activities has grown significantly, which has increased the need for information security audit. It should be noted, however, that information audit activities are regarded by corporations and organizations as passive additional work procedures that unnecessarily increase the workload of their employees; thus, the necessity of information audit activities has been accorded insufficient importance. Vladimir (2020) opined that the effectiveness of an information system's controls is evaluated through an information systems audit. An audit aims to establish whether information systems are safeguarding corporate assets, maintaining the integrity of stored and communicated data, supporting corporate objectives effectively, and operating efficiently. It is a part of a more general financial audit that verifies an organization's accounting records and financial statements.

Information security audit have been defined and classified in a number of different ways and subsequently, there is no widespread agreement on their definition or classification. Studies have identified various strategies such as deterrence, prevention, surveillance, detection, response, deception, perimeter defense, compartmentalization and layering. Data integrity refers to protection of information from being modified by unauthorized parties. Information is only valuable when it has not been tampered with. Information that has been altered inappropriately could prove costly, for example if you made a transaction of ₦1,000 and someone altered it to ₦100,000. Protecting data from tampering by unauthorized persons is paramount in information security (Ocharo, 2014). Availability of information refers to ensuring authorized people have access to the information as and when needed. Denying the rightful users access to information is quite a

common attack in this internet age. Users can also be denied access to data through natural disasters such as floods or accidents such as power outages or fire. The key to ensuring data availability is back-up. Backed-up data should ideally be stored at a location far away to ensure its safety, but this distance should take into account the time it would take to recover the backed-up data. An information systems audit would therefore ensure that the organization's data is confidentially stored, that data integrity is ensured and data is available at all times for the authorized users. An information systems audit is an audit of an organization's information security audit systems, management, operations and related processes.

Despite the spread of awareness of the importance of information system integrity, little investment in information security audit is made even now, thereby making it difficult for office administrators to effectively engage in information protection and other administrative activities that is required of their office. Moreover, in a corporation or corporate institution, audit activities are regarded as a factor that leads employees to complain about their jobs, thereby hampering the derivation of a direction for improving information security activities (Kim, 2013). Hence, information security audit is an issue of concern for institutions. At all levels, whether small, medium or large, sole proprietorship, partnership or company, security remains a priority (Anderson, 2011). For institutions to survive and remain competitive in the contemporary turbulent environment, management of security has to be done efficiently (Ndung'u, 2014). Despite the rapid changes and enhancements of management information systems practices, a number of firms still rely on old systems to manage their information.

Effective information security strategy is key to meeting business challenges. By treating IS as an enabler of manageable, accountable and scalable access, the protection of the information system's integrity becomes the catalyst for safe and open information exchange. From this perspective information security audit is no longer just a straight cost but rather an investment in business growth and development. In addition, information security audit has become the vehicle by which new business opportunities are realized and enables business continuity. Information resources play a critical role in sustaining business success by driving innovation and opportunities for the development of competitive advantage. As such, preservation of the confidentiality, integrity and availability of these information resources is a significant imperative for organisations, as is the need for a viable information security audit in organisations to facilitate information transfer at an inter-organisational level. State-owned universities have come to appreciate the roles and importance of Information security audit, and the need to provide necessary technologies and approaches to facilitate improved administrative outcome. This assertion is in consonance with Frost and Sullivan (2013) that the safety and efficiency of these systems may affect the stability and soundness of the managerial and financial institution of organizations and consequently their profitability, productivity and decision making. As such, safeguarding the integrity of the systems is perceived to improve administrative effectiveness of institutions. Information security audit is a perceived roadmap for information and information infrastructure protection with goals and objective that ensure capabilities provided are aligned to business goals, there is need to ascertain with empirical evidence the relationship between information security audit and administrative effectiveness. It is against this background that this study is prompted.

Statement of the Problem

In today's world, there is a growing need for improved effectiveness in terms of problem solving, service delivery and actionable decision making. The necessity for effectiveness increases on daily basis and thus becomes more complex in nature. Also, as organization keeps growing, the management, staff and other users within and outside the organization continues to depend and demand for sophisticated technology-oriented information system to support the administrative duties and operations of the organization. Such information required should be accurate, timely and aimed at the correct recipients. In view of this, the researcher attempts to establish the manifestation of information security auditing and the significant relationship between information

security auditing and organizational effectiveness. Also, business managers are becoming increasingly aware that information security audit can be used to produce meaningful information on which they can base their service delivery in addition to performing the detailed creative functions of the organization.

In spite of the foregoing, there appears to be a limited level of information ssecurity audit in the state-owned universities in Nigeria which has led to incessant cases of online result alteration, falsification of online data, online administrative information spy, phishing, social engineering, hacking of information as well as accounts, etc. In recent time Swedish Financial Supervisor Authority noted that Cyber security incidences have increase frequently over the years especially in Nigeria, if this trend is not checked or left unabated it will cripple the integrity of our tertiary institution's information system as well as related organizations.

Moreover, the importance of the state-owned universities as an aspect of the information system has been neglected over the years as most studies on the interaction between the information security auditing and effectiveness has focused mainly on the banks, insurance firms, manufacturing firms, SMEs and the stock market. However, recently, growing attention has shifted to the interaction between the educational intermediaries such as the state-owned universities. Nevertheless, the researcher as at the time of this study observed that no local study focused on information security audit and administrative effectiveness in state-owned universities which is an identified nexus in existing literature. Therefore, there is need to close this knowledge gap.

Conceptual Framework

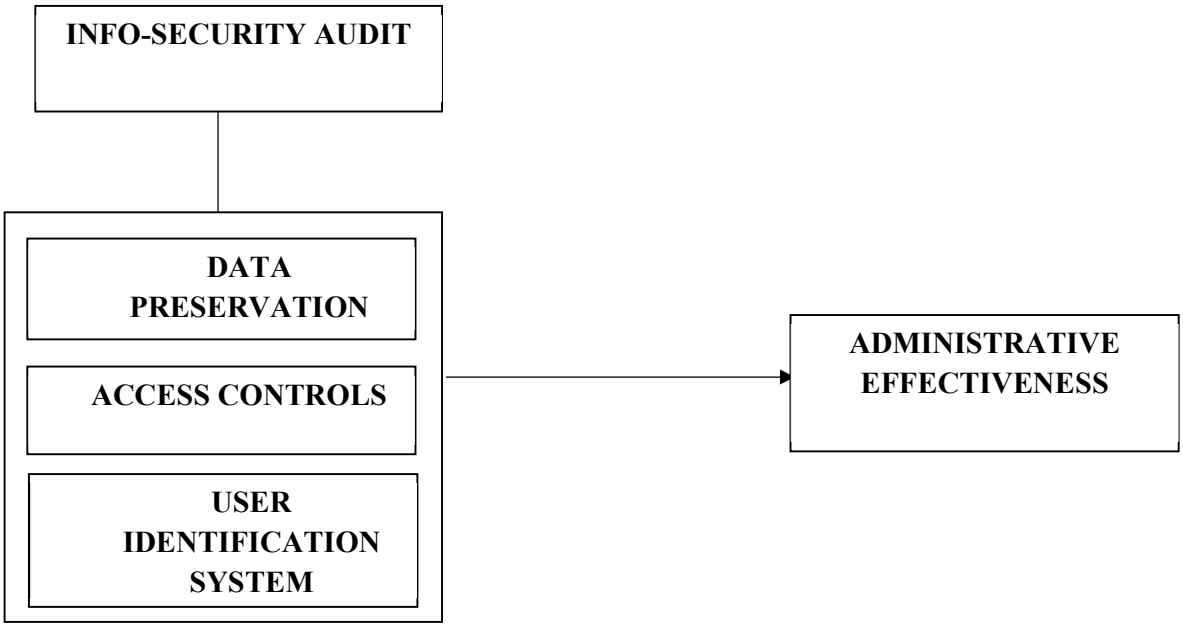

Fig 1.1 Conceptual Framework on Information security Audit and Administrative Effectiveness

Source: Researcher's Conceptualization (2021); Grusovink et al. (2017), Mohammadi et al. (2012)

Aim and Objectives of the Study

The purpose of this study was to determine the extent to which information security audit correlate with administrative effectiveness in state-owned universities in Rivers State. Specifically, the objectives of the study are:

1. To determine the extent to which data preservation correlates with administrative effectiveness in state-owned universities in Rivers State.

2. To determine the extent to which access control correlates with administrative effectiveness in state-owned universities in Rivers State.
3. To examine the extent to which data user identification system correlates with administrative effectiveness in state-owned universities in Rivers State.

Research Questions

In order to achieve the stated objectives, the following research questions are set:

1. To what extent does data preservation correlate with administrative effectiveness in state-owned in Rivers State?
2. To what extent does access controls correlate with administrative effectiveness in state-owned universities in Rivers State?
3. To what extent does user identification system correlate with administrative effectiveness in state-owned universities in Rivers State?

Research Hypotheses

The following null hypotheses are formulated to guide the study:

H_{o1}: There is no significant relationship between Data preservation and administrative effectiveness in state-owned universities in Rivers State.

H_{o2}: There is no significant relationship between access controls and administrative effectiveness in state-owned universities in Rivers State.

H_{o3}: There is no significant relationship between user identification system and administrative effectiveness in state-owned universities in Rivers State.

Theoretical Framework

In this research work, for empirical analysis and understanding, general system theory was adopted as a theoretical underpinning to this study. The system theory was propounded by a renounced biologist Von Bertalanffy (1972) which is applied in analysis of business organizations. In other words, the system theory depict business organization as a 'whole' that has component parts, that interact with one another to achieve overall objective of the organization while no part or component of the entire system is insignificant.

Since information systems audit represents an interdisciplinary study of the structure of regulatory systems, it refers to the study of how actions by a system cause changes in the environment that are understood by the system itself in terms of feedback, allowing the adaptation of the system to new conditions. In other words, the system can change its behavior. In information systems, the system and the environment present different levels of complexity, as the environment has degrees of complexity that are not perceptible to the system (Golinelli et al, 2002; Barile, 2006).

METHODOLOGY

The study adopted a research survey design to assess the correlation between information security audits and administrative effectiveness in state-owned universities in Rivers State. Descriptive survey design was used for this study because it determines and reports the way things are describing as well interprets what the data is.

The population for this study comprised of two hundred and ninety-sixty (296) administrative staff of the two state-owned universities in Rivers State. These are regarded in this study as the three levels of administrative staff(s) such as Senior Management, Middle Management and Low management. To avoid misunderstanding between the positions held in different institutions.

For this study, the researcher conducted census survey and as such there was no sample size drawn from the population. Census survey is a complete listing of all the items in the population. It is studying the entire population without drawing a sample size. The sampling technique for the study was the census sampling techniques. It is a type of sampling technique in which the researcher decides to study the whole population that possess the particular set of characteristics

e.g. knowledge, experience, etc. The sample size for this study was 260 office and information managers in the two state-owned universities.

The study used questionnaires to collect primary data from the respondents. Two sets of questionnaires used were titled Information security audits Questionnaire (ISAQ) and Administrative Effectiveness Questionnaire (AEQ). The questionnaire was divided into different sections and each section aimed at addressing a particular objective of the study. The instruments was designed along the 5-point Likert rating scale of Very High Extent = VHE, High Extent = HE, Moderate Extent = ME, Low Extent = LE and Very Low Extent = VLE. The responses were scored as follows: Very High Extent = VHE, High Extent = HE, Moderate Extent = ME, Low Extent = LE and Very Low Extent = VLE respectively.

To validate the instrument, the questionnaire was given to the researcher's supervisor and other experts from the department of office and information management and test and evaluation experts who read through, checked for content and face validity and made necessary corrections which were noted and effected before the administration of the instrument to the respondent's necessary corrections.

The strength of the instrument used in this study was subjected to reliability to elicit the required information concerning recruitment strategies and organizational performance. However, the true measure of the reliability of the instrument was based on statistical data. Reliability of the questionnaire was evaluated through Cronbach's Alpha test which measures the internal consistency. Cronbach's alpha was ascertained by utilization of SPSS version 26 for unwavering quality analysis. A reliability coefficient of 0.89 was obtained. The questionnaire was analyzed using Statistical Package for the Social Sciences (SPSS) Version 23: Mean, and Spearman ranked correlation was the means of analysis.

RESULTS

Out of the 296 copies of questionnaires distributed to the respondents, 291 which represent 98.3% of the sample were duly filled and returned. The analysis further revealed that a total of 5 copies of questionnaire representing 1.7% of sample were not returned. This is further illustrated in Table 4.1.

Table 4.1 Administration of Instrument

QUESTIONAIRE ALLOCATION	RESPONDENTS	%
Filled and Returned	291	98.3
Unreturned	5	1.7
Total Distributed	296	100

Source: Study data, 2021

The results of three (3) hypothesis were analyzed using Spearman Rank Correlation Coefficient (rho). The strength of the correlation is determined following the rule:

Coefficient Value	Strength of Association
$0.1 < \| rho \| < .19$	Very weak correlation
$0.2 < \| rho \| < .39$	Weak Correlation
$0.4 < \| rho \| < .59$	medium/moderate correlation
$0.6 < \| rho \| < .79$	Strong correlation
$\| rho \| > .79$	Very strong correlation

H_{o1}: There is no significant relationship between Data preservation and administrative effectiveness in state-owned universities in Rivers State.

Table 1: Analysis of Relationship Between Data preservation and administrative Effectiveness

			Data Preservation	Administrative Effectiveness
Spearman's rho	Data Preservation	Correlation Coefficient	1.000	.722**
		Sig. (2-tailed)	.	.000
		N	291	291
		Remark		Strong positive relationship

**. Correlation is significant at the 0.01 level (2-tailed)

Source: SPSS Output from Field Data (2021)

Table 2 showed that Data preservation when compared against administrative effectiveness yielded rho values of 0.722. The result showed that there is a strong relationship between Data preservation and administrative effectiveness (rho = .722, p = 0.000). Based on these results the null hypotheses are all rejected. Hence there is a significant relationship between Data preservation and Administrative effectiveness in the universities in Rivers State.

H_{o2}: There is no significant relationship between access controls and administrative effectiveness in state-owned universities in Rivers State.

Table 2: Analysis of Relationship Between access controls and administrative Effectiveness

			Access Controls	Administrative Effectiveness
Spearman's rho	**Access Controls**	Correlation Coefficient	1.000	.680**
		Sig. (2-tailed)	.	.000
		N	291	291
		Remark		Strong positive relationship

**. Correlation is significant at the 0.01 level (2-tailed)

Source: SPSS Output from Field Data (2021)

Table 2 showed that access controls when compared against administrative effectiveness yielded rho values of 0.680. The result showed that there is a strong relationship between access controls and administrative effectiveness (rho = .680, p = 0.000). Based on these results the null hypotheses are all rejected. Hence there is a significant relationship between access controls and administrative effectiveness in the universities in Rivers State.

H_{o3}: There is no significant relationship between Data preservation and administrative effectiveness in state-owned universities in Rivers State.

Table 3: Analysis of Relationship Between user identification system and administrative Effectiveness

			User Identification System	Administrative Effectiveness
Spearman's rho	**User identification system**	Correlation Coefficient	1.000	.559**
		Sig. (2-tailed)	.	.000
		N	291	291

Remark	Moderate positive relationship

**. Correlation is significant at the 0.01 level (2-tailed)

Source: SPSS Output from Field Data (2021)

Table 3 showed that Data preservation when compared against administrative effectiveness yielded rho values of 0.559. The result showed that there is a strong relationship between user identification system and administrative effectiveness (rho = .559, p = 0.000). Based on these results the null hypotheses are all rejected. Hence there is a significant relationship between user identification system and administrative effectiveness in the universities in Rivers State.

DISCUSSION OF FINDINGS

The investigation of the relationship between Info-security audit and administrative effectiveness followed three specific hypotheses that were tested. These hypotheses (Ho_1, Ho_2 and Ho_3) were rejected based on the emerging p-values less than 0.05. The results revealed very weak to very strong positive relationship between Info-security audit and measures of administrative effectiveness. The result obtained in the study was as follows:

Ho_1: Data preservation has a very strong positive relationship with administrative effectiveness in state-owned universities, Rivers State (rho = 0.722; p = 0.000).

Ho_2: Access controls has a strong positive relationship with administrative effectiveness in state-owned universities, Rivers State (rho = 0.680; p = 0.000).

Ho_3: User identification system has a moderate positive relationship with administrative effectiveness in state-owned universities, Rivers State (rho = 0.559; p = 0.000).

Summarily, the result revealed significant relationship between Info-security audit and administrative effectiveness. It showed that Info-security audit has tendencies to improve the problem solving, service delivery and decision-making in state-owned universities in Rivers State. This means that poor usage of Info-security audit will also result in poor performance of office managers. These findings agree with Gupta (2015) that Info-security audit is useful in students' assessment and grading. Pupescu et.al. (2018) was security audit is essentially an assessment of how effectively the organization's security policy is being implemented.

It is done with a view to improve those activities, uncover shortcomings and address the deficiencies so that firms can perform better within an increasingly diverse range of technologies as an essential part of learning and teaching in the 21st century. He further asserted that information security audit constitutes an input in the administrative process that helps produce better administrative output. The availability of information security audit can enhance effective office management by making education less dependent on differing teacher quality and by making education available at home throughout the day.

CONCLUSIONS

This study was primarily carried out to determine the extent to which information security audit correlate with administrative effectiveness in state-owned universities, Rivers State. The research uncovers consequences and usefulness of information security audit in an organization. Businesses have major goals that include increase in profit, larger market share, counter competition and brand identity process. In order to achieve these goals, institutions must rely on constant flow of information. The findings also revealed that information security audit is very important for improving administrative effectiveness in the organizations. Thus, the study provided an insight into the relevance of information security audit on administrative

RECOMMENDATIONS

Based on the findings of the study and conclusions drawn from the study, the following recommendations are made:

1. Tertiary institutions should strengthen information technology (IT) information resource audit practices more so as to improve the effectiveness of its administrative function to a very great extent.
2. Management of the universities are highly encouraged to develop a clear strategy to allow for increased role of general controls of information security system in improvement of their problem solving and decision-making process.
3. The attention of office managers in your institution should be directed towards the use of Information Technology in routine office as to improve on the institutions' information security audit.

REFERNECES

Chang, J.C.J. & King, W.R. (2005). Measuring the performance of information systems: A functional scorecard. *Journal of Management Information Systems, 22*(1), 85-115.

Chu W. (2015). MIS problems and failures: A socio-technical perspective, part ii: the application of socio-technical theory. *MIS Quarterly, 1(*4), 11.

Chu W. (2015). MIS problems and failures: A socio-technical perspective, part ii: the application of socio-technical theory. *MIS Quarterly, 1(*4), 11.

Eden, C. (2016). Managers, computer systems, and productivity. *MIS Quarterly, 5*(3), 1-20.

Tang, J. & Chamberlain, A. (2017). An integrated system theory of information security management. *Information Management & Computer Security, 11*(5), 243–248.

Whitman, S.D., Horne, C. A., Ahmad, A., & Maynard, S. B. (2014). A theory on information security. *Australasian Conference on Information Systems, 3*(8), 1–12.

Xiao, L. & Cao, S. (2017). *The relationship between information technology and corporate financial reporting.* http://www.emeraldinsight.com.

Vladimir, H. (2020). A review of information security issues and respective contributions. *The Data Base for Advances in Information Systems, 38*(1), 60–80.

Ndung'u, A. (2014). Strategic planning for information systems, (3rd ed). John Wiley & Sons Ltd.

Anderson, R. (2011). *Changing information technology and it audit.* Sanei Press

Frost, T.& Sullivan, M. (2013). Revisiting the information audit: A systematic literature review and synthesis. *International Journal of Information Management 37*(1), 1380–1390