DESCRIPTIVE OF QUANTITATIVE DATA | SUPPLEMENTARY

Logical Environment and Supervisory Regulatory Frameworks for Effective Information Management of Public Universities in Nigeria

Janet Achikere Onimawo[1], Friday Ekahe Abanyam[2*], Fabian Ugbe Udida[3], Anthonia Ngozi Ibelegbu[4], Judith Kanu[5]

[1] Department of Public Administration, Faculty of Management Sciences, Ambrose Alli University Ekpoma, Edo State, Nigeria. Email: achijane@aauekpoma.edu.ng
[2*] Department of Business Education, Faculty of Education, Ambrose Alli University, Ekpoma, Edo State, Nigeria, Email: fabanyam@aauekpoma.edu.ng
[3] Department of Vocational Education, Faculty of Education, University of Calabar, Cross River State, Nigeria. Email: fabianudida@gmail.com
[4] Department of Vocational and Technology Education, Taraba State University, Jalingo , Taraba State, Nigeria.Email: ibelegbungozi@gmail.com
[5] Nigeria Educational Research and Development Commission (NERDC), Abuja, Nigeria. Email: kanujudith8@gmail.com

Abstract: The study determined the logical environment and supervisory regulatory frameworks for effective information management of public universities in Nigeria. The study adopted descriptive survey research design. The population was 1580 Management staff. 432 respondents were proportionally sampled from each of the Public universities studied. The instrument for data collection was a structured questionnaire developed by the researcher. The questionnaire was face-validated by five experts. The reliability of the instrument was tested using Cronbach Alpha method and yielded an overall coefficient of 0.93. Mean and Analysis of Variance were used to analyze data collected. The findings showed that the management staff agreed to the 42 items measuring the logical environment and Supervisory regulatory actions for effective information management. The findings further showed that no significant difference existed among the opinions of the respondents on the level at which they adopted the logical environment security and supervisory regulatory actions for effective information management of their institutions. It was recommended among others, that the management of Public universities in Nigeria should enact and implement effective policies and laws that support the adoption of information regulatory actions.

Keywords: Logical Environment, Supervisory Control, Regulatory Framework, Information Management, Public Universities

1. Introduction

Public university management structure in Nigeria was set up amongst other goals to prepare individuals to become leaders and practitioners in every area of human endeavor in order to expand and deepen understanding of education as a fundamental human right. To achieve these goals therefore, the management needs the right information at the right time and in the right form, which is usually processed by the management staff in various capacities as supportive staff in the administration of the university system.

Management staff, across all public universities in Nigeria, deals with the gathering, processing and communication of information. They also maintain effective oral and written communication processes between the college management and other levels of staff with regard to fiscal and other matters. According to Naboth-Odum, Abanyam, Abdulkadir and Abanyam (2022), management staffs are the greatest resource of Public universities because they make critical difference in the ability of the colleges not to merely survive, but to thrive. To be truly effective, the design, practices and policies of Public universities must be beneficial from the way management staff process information. In `management, there are three major classifications of managerial levels, namely: strategic, tactical

and operational levels (Jumper, 2005; Martin, 2011; Mikoluk, 2013). This classification is based on functions and responsibilities of the management staff.

There are diverse categorizations of management levels. As posited by Nabort-Odums et. al. (2022), management levels are customarily characterized as strategic, tactical and operational. Strategic mangers are top-level managers, tactical managers are the middle-level managers, while the operational managers are the low-level managers. According to the authors, while the strategic managers are concerned with the planning functions of an organization, policy formation and development of long-term goals of the entity, the tactical level managers carry out the visions of the top-level managers by coordinating both human and material resources to achieve the organizational goals. The primary responsibility of the tactical managers is organizing, coordinating and staffing. On the other hand, the operational managers are the supervisors. They direct, regulate and monitor staffs to carry out needed activities of the organization. They also required to check workers' attendance, maintain quality regulatory, handle complaints, track schedules, cost, and ensure effective and efficient maximization of workers input to duty (Mikoluk, 2013). The degree of success of any educational institution depends on the extent to which the management staff are able to manage the information systems.

Information management (IM), as stated by State of Vermont (2015), involves all the basic attributes of management including: planning, organizing, structuring, processing, evaluation and reporting of information activities, all of which must be regulated strategically. Thus, IM in this study is is a cycle of organizational practices that have to do with the creation, distribution, storage, and making such information available to those in need of such information as well as the final disposition of such records with the objectives of accomplishing the institutions' set goals. As such, State of Vermont (2015) posits that for an institution to effectively operate and regulate their information system, they must ensure that such IM structure must be relevant, valid, reliable, and timely. Therefore, Management staff are required to make available reliable information for optimal management decisions and communicate regulatory decisions to those in need of them. Effective IM must apply certain regulatory actions to ensure proper processing, securing and timely delivery of information.

Several management regulatory actions that can be adopted by educational institutions in Nigeria, have been proposed by different experts, but the complexity with which they operate varies in line the peculiarity of their institutions. Never the less, management regulations are classified as procedural preventive and detective Actions (McCrindell, 2015; State of New York Comptroller, 2007); logical security and environmental controls (Mattie, Hanley & Cassidy, 2005); storage, information communication, environment (physical), and supervisory actions (Gauthier, 2014) The Institute of Internal Auditors, 2008); and recovery controls (Fabunmi, 2006). In this study however, logical environment and supervisory regulations shall be of interest to the researchers.

The logical environment regulations set the tone of an organization, influencing the regulatory consciousness of its people. Abanyam, Ibelegbu and Garba (2020) defined environment as those peripheral elements that sway the system as a result of changes in their behaviour, or properties. The regulatory environment is influenced by institutional philosophy, operating style, integrity, ethical values, and commitment to competence. If the regulatory environment is positive, the overall system of information management will be more effective. In the view of Abanyamm and Abanyam (2021) and Misra, 2019), environmental regulatory measures could be looked at from three regulatory principles, namely: principle of standard, principle of measurement of performance against standard, and principle of corrective action. The authors explained that the principle of standard demands that standard should be set for all activities relating to information management. The accepted standard should be clearly and precisely enough for all tasks of the organization including the information management systems. The principle of management of performance against standard stated that standards are useless unless actual performance is measured and compared against the standard. The principle of corrective action states that when measurement of performance indicates that a standard is not being met, appropriate correction should be taken (Ibelegbu & Abanyam, 2022; Northcutt,

2009). Hence, failure to correct what is wrong leads to waste of human, material, and information resources.

The regulatory system requires to be monitored, in order to assess whether regulations are effective and is operating as intended. According to State of Vermont (2015), supervisory occurs through routine managerial activities such as supervision, reconciliations, checklists, comparisons, performance evaluations, and status reports; supervisory may also occur through separate internal evaluations or from use of external sources. Institute of Internal Auditors (2008) posited that deficiencies found during supervisory require to be reported to those responsible for the function, with serious deficiencies being reported to top management. If an effective continuous supervisory program is in place, it supports effective information recovery required to maintain effective information management. The demand for effective information security measure is an urgent need in tertiary institutions across the world. This is because there are several cases of attacks occurring on daily basis on institutional information systems (Misra, 2019). According to Mellon (2013), there are about 90,000 to 100,000 cyber attempts and attacks per day on institution's websites. The author lamented that such attacks have resulted in a lot of data breach of several staff and students. In Nigeria, several of such attacks have been observed. According to Egwu (2016), as of 2016, Nigeria is ranked 16th highest country in cyber-attacks vulnerabilities in Africa.

Several tertiary institutions, including Public universities in Nigeria and other Africa countries have suffered cyber attacks. According to a Report by Naboth-Odums et. al. (2022) and Africa Cyber Security (2016), most African countries have lost more than US$2 billion in cyberattacks in 2016 only. Similarly, researchers have found that there are numerous incidences of cybercrimes and fraudulent activities against tertiary institutions' websites, digital documents, databases and networks in Nigeria and particularly in the study area (Rogers & Ashford, 2015). The authors lamented that cybercrimes and hacking activities have caused several tertiary institutions in Nigeria billions of Nigeria unfortunately very few of the tertiary institutions have made efforts to ameliorate the root cause of the attack. The causes of the attack are as a result of poor information regulatory actions, failure to patch and secure institutional information systems. Based on this background, it is very salient that management of Public universities in Nigeria put in place good information regulatory actions to safeguard their institutions from unforeseen hack and cyberattacks. It is against this background that the present study sets to determine the logical environment and supervisory regulatory frameworks for effective information management of public universities in Nigeria.

2. Related Empirical Studies

AbdulAzeez (2016) carried out a study on analysis of management practices in Lagos State tertiary institutions. Using a population of 905 academic and non-academic staff and final year students of the institutions, the study found a significant positive relationship between quality teacher education and total quality management practices in both public universities and universities in Lagos State. Furthermore, Wynn (2017) explored the relationship between information security success factors and the organization's information security culture. Employing a population of 140 Information Technology Professionals, the results revealed that correlations exist between information security success factors and the organization's information security culture.

In addition, François (2016) carried out a study on the relationship of information security policy awareness, enforcement, and maintenance to information security program effectiveness. The population of the study was 119 volunteers. This study used multiple regression analysis to predict values of the dependent variables. The study found that the independent variables such as total policy awareness, total policy enforcement, and total policy maintenance were statistically significant predictors of the level of total program effectiveness. In another vein, Okolo (2015) conducted a study on evaluating factors of security policy on information security effectiveness in developing nations. Using a population of 72 information security professionals, the study found a high positive relationship between security policy awareness and security program effectiveness as well as a high and

positive relationship between security policy maintenance and security information program effectiveness in Nigeria.

The reviewed literature revealed that information supervisory and logical environment regulatory measures are the foundation of the internal information system for managers. It provides that management needs to plan and regulatory the institutions' activities. Again, several researches showed that management office operation is an integral part of any organization. Authors are also in agreement that management department in any institution is the backbone of the organization. Similarly, management staff of the public universities are in charge of the management office operations. The administrators should as well be able to develop an appropriate and up-to-date office and assets management strategies, and should be able to also develop good management procedures. They should be able to apply management regulatory measures for effective information management.

In addition, literature has shown that information management has received serious attention in the last few decades and a lot of contemporary issues come into information profession. The authors reviewed stressed that in the dynamic world of industry, business, and education, information management is never static but always changing for greater efficiency. The literature also revealed that the global visibility of the academic activities and ability to manage digital, offline information and assets have much to tell about the quality, and the ranking of an educational institution. This has increased the need for effective information management through an adequate internal regulatory measure. Furthermore, literature revealed that good information regulatory measure will assist institutions to mitigate any unforeseen threat from attackers and information fraudsters. The researchers also reviewed The Fraud Triangle Theory by Donald Cressey that supports the study. Finally, several related empirical studies were reviewed. Although the reviewed empirical studies have some similarities with the present study, none of them or any other known to the researchers was on logical environment and supervisory regulatory frameworks for effective information management of public universities in Nigeria. Hence, we f formulated and tested the following hypotheses for the study:

1. There is no significant difference in the mean responses of strategic, tactical, and operational management staff on the logical environment regulatory actions adopted for effective information management.
2. There is no significant difference in the mean responses of strategic, tactical, and operational management staff on the supervisory regulatory actions adopted for effective information management.

3. Research Method and Materials

This study adopted descriptive survey research design. Descriptive survey design is one in which a group of people or items are studied by collecting and analyzing data from only a few people or item considered to be representatives of the entire group (Abanyamm & Guma, 2021). This design is therefore considered suitable for this study because it makes use of questionnaire to collect data from the respondents on logical environment and supervisory regulatory frameworks for effective information management of public universities in Nigeria. There have been several reports of cybercrimes and hacking activities against educational institutions' databases and networks in the area. Most tertiary institutions in the area express that they witness various breaches of information however, which they hardly identify when the attack is attempted until much later when it has done serious harms on the institutions.

The population for the study was 1,580 consisting of 232 strategic, 569 tactical and 779 operational management staff of Public universities in Nigeria. The sample size of the study was 320 respondents from 12 (6 State and 6 Federal) Public universities across the six Geo-political Zones that make up Nigeria. Taro Yamene's formula in Abanyam (2014) was used to determine the sample size of 432 respondents from the Public universities being studied. After determining the sample size, proportionate sampling technique was used to determine the number of the strategic, tactical and

operational management staff for each of the Public universities studied. The strategic, tactical, and operational management staffs were chosen because they are the main information management staff of the Public universities. Again, they possess the experience and expertise needed for effective information management therefore, were in good position to respond to questions about the logical environment and supervisory regulatory frameworks for effective information management.

The instrument used for data collection was structured questionnaire titled "logical environment and supervisory regulatory frameworks for effective information management (LESRFEIM)" developed by the researchers. The questionnaire sought information on the logical environment security and supervisory regulatory frameworks for effective information management of public universities in Nigeria in Public universities with 22 and 20 items respectively and was structured on a 4-point scale with response options of strongly agree, agree, disagree and strongly disagree with weights of 4, 3, 2, and 1 respectively.

The questionnaire was face-validated by five experts and trial-tested on a sample of 30 management staff. From each of the 6 Geo-political Zones, 5 Management staffs in Colleges of Education in Nigeria randomly selected for this study. Cronbach Alpha reliability method was used to determine the internal consistency of the instrument which yielded 0.96 for logical environment security and 0.93 for supervisory regulatory frameworks with an overall coefficient of 0.93.

The researchers with the help of twelve (12) research assistants, one for each of the 12 Federal and State Public universities in Nigeria administered the questionnaire to the respondents. We found it difficult to get responses from some strategic management staffs who blatantly objected to out request of provide information for this study, notwithstanding recurring visits and encouragements. Moreover, some of the respondents were motivated to participate since they were not interest in providing response to the questions raised for the study. Consequently, the indifference to answer to the questionnaire items by some respondents couple with our inability to obtain qualitative information from some of needed the respondents would affect the generalization and validity of this research. However, we were able to deal with these challenges by persuading and pacifying some of them with gift items, which spur their interest to participate in the study. Hence, four hundred and thirty two (432) copies of the questionnaires were distributed to the respondents, but three hundred and eighty (392) indicating a returned rate of 87.5% of the respondents who correctly filled all aspects of the questionnaires and were retrieved after a period of one week. were used for the data analysis (i.e. Strategic management staff (SMS)=82, tactical management staff (TMS)=133, operational management staff (OMS)=177).

Analysis of data was carried out using both quantitative and qualitative statistical tools such as mean, standard deviation and Analysis of Variance (ANOVA). The real boundary of numbers technique was used to interpret the outcome of data analyzed on the mean as shown in Table 1.

Table 1: Real boundary of numbers for mean interpretation

Serial number	Response options	Values	Point Boundary Limit
1	Strongly Agreed (SA)	4	3.0 – 4.0
2	Agreed (A)	3	2.0 – 2.9
3	Disagreed (D)	2	1.0 – 1.9
4	Strongly (SD)	1	0.0 – 0.9

Also, to test hypotheses, the hypothesis of no significant difference was not rejected if the p-value was higher than or equal to 0.05 level of significance. On the other hand, where the p-value was lower than the significance level of 0.05, the null hypothesis was rejected.

4. Research Method and Materials

This section presents the analysis of data collected for the study. The analysis is presented according to the research questions and the hypotheses that guided the study.

4.1. Hypothesis One

Table 2: ANOVA of the mean responses of management staff on the logical environment regulatory actions adopted for effective information management

| | The Logical environment regulatory action (LESCA) | Nos of SMS = 82, TMS = 133, OMS = 177 Total respondents = 392 | | | | | | | |
		$\bar{x}_{SMS}$	$\bar{x}_{TMS}$	$\bar{x}_{OMS}$	Remarks	Df	F-ratio	P-value	Rmk
1	Set up regulatory activities that will help to mitigate risks.	3.27	3.22	3.17	SA	390	5.89	0.00	S
2	Maintain accountability standard for the execution of internal regulatory responsibilities.	3.34	3.13	3.40	SA	390	1.75	0.18	NS
3	Deploy regulatory activities that are in line with policies and procedures of the institution.	3.22	3.30	3.10	SA	390	1.13	0.32	NS
4	Communicate internal regulatory deficiencies.	3.45	3.17	3.29	SA	390	6.07	0.00	S
5	Communicate internal regulatory information internally.	3.26	3.29	3.28	SA	390	0.45	0.64	NS
6	Set up standard code of conducts to maintain ethical values	3.55	3.34	3.16	SA	390	2.45	0.09	NS
7	Identify and analyze risks	3.29	3.20	3.23	SA	390	6.21	0.00	S
8	Use internal audit and/or compliance function to assessing and maintaining institution's regulatory environment.	3.28	3.34	3.26	SA	390	12.16	0.00	S
9	Perform ongoing or periodic evaluations of internal regulations (or a combination of the two).	3.55	3.23	3.18	SA	390	5.38	0.01	S
10	Communicate internal regulatory strength to maintain.	3.38	3.25	3.33	SA	390	4.21	0.02	S
11	Use incentives to motivate staff to ensure environmental security of the institution's information resources.	3.29	3.21	3.13	SA	390	14.98	0.00	S
12	Employ personnel with the experience and skill-sets specific to information management and security.	3.34	3.27	3.18	SA	390	2.70	0.07	NS
13	Maintain collaboration in the oversight of internal regulatory activities of staff	3.45	3.27	3.13	SA	390	17.77	0.00	S
14	Establish authority and reporting structure to	3.38	3.21	3.14	SA	390	8.58	0.00	S

	The Logical environment regulatory action (LESCA)	Nos of SMS = 82, TMS = 133, OMS = 177 Total respondents = 392						
		$\overline{x}_{SMS}$	$\overline{x}_{TMS}$	x_{OMS}	Remarks	Df	F-ratio	P-value	Rmk
	achieve logical environment objectives.								
15	Specify appropriate objectives to support effective environmental regulatory mechanisms.	3.45	3.19	3.22	SA	390	1.57	0.21	NS
16	Identify and analyze changes that could significantly affect internal regulations	3.35	3.17	3.25	SA	390	0.95	0.39	NS
17	Demonstrate a commitment to attract, develop, and maintain competent staff through constant trainings on information management.	3.28	3.21	3.20	SA	390	9.16	0.00	S
18	Evaluate fraud risks in the information systems.	3.37	3.22	3.09	SA	390	8.17	0.00	S
19	Develop technology regulations to ensure that information systems are often checked against errors and malfunctioning.	3.23	3.24	3.30	SA	390	0.32	0.73	NS
20	Use relevant, quality information to support the internal regulatory function.	3.23	3.14	3.09	SA	390	6.64	0.00	S
21	Communicate internal regulatory information externally.	3.32	3.20	3.42	SA	390	1.73	0.18	NS
22	Engage external entities to provide management with accurate picture of the institution's regulatory environment.	3.45	3.21	3.18	SA	390	4.87	0.01	S
	Cluster mean	3.28	3.13	3.13	SA	390	5.60	0.13	NS

Key: xSMS = Means of Strategic Management staff, xTMS = Means of Tactical Management staff, xOMS = Means of Operational Management staff, Rmk = Remark, NS = Not Significant, S = Significant

The result in Table 2 showed the mean ratings of the respondents on the logical environment regulatory framework for effective information management of public universities in Nigeria. The result showed mean ratings of the items to be above 3.0 indicating that the Management staff strongly agree that the listed 22 items are logical environment regulatory actions. In like manner, the corresponding standard deviation to each of the items ranged from 0.11– 0.49 with an overall of 0.45, signifying that the opinions of the respondents were very close to one another on the level at which they agreed to the logical environment regulatory actions.

Table 3 also showed the ANOVA result of the hypothesis of no significant difference among the mean responses of Strategic, Tactical and Operational Management staff on logical environment regulatory framework needed for effective information management of Public universities in South-South Nigeria. The item-by-item analysis showed that the hypothesis was not significant on items 1, 5, 6, 9, 11, 12, 14, 15, and 20 and the overall mean, whereas items 1, 4, 6-14, 17-18, 20, and 22 are

significant. Although the result shows significant and non-significant differences on the items, since the cluster value (P-value) is 0.13, the null hypothesis (Ho1) was not rejected.

4.2. Hypothesis Two

Table 3: ANOVA of the mean responses of management staff on the supervisory regulatory framework for effective information management

| | The Supervisory Regulatory Framework | Numbers of SMS = 82, TMS = 133, OMS = 177 Total Respondents = 392 | | | | | | |
		$\overline{x}_{SMS}$	$\overline{x}_{TMS}$	$\overline{x}_{OMS}$	Rmk	Df	F-ratio	P-value	Rmk
1	Critical observation of all important aspects of the institution's information centers	3.10	3.12	3.32	SA	278	3.29	0.04	S
2	Specify a standard of satisfactory performance in service delivery	3.09	3.09	3.29	SA	278	0.56	0.57	NS
3	Ensure strict authorization and verifications of all institution's data and files to be shared	3.28	3.09	3.11	SA	278	2.44	0.09	NS
4	Specify the type of data comparisons to be made if performance is outside the range.	3.42	2.97	3.08	SA	278	2.24	0.11	NS
5	Identify the stages of each information process	3.18	3.08	3.13	SA	278	8.11	0.00	S
6	Clearly state the key inputs and outputs stages of each information process	3.29	3.12	3.15	SA	278	2.24	0.11	NS
7	Assign capable staff to man the monitoring unit	3.33	3.16	3.18	SA	278	2.38	0.09	NS
8	Set special monitoring activities in high-risk information areas	3.26	3.23	3.22	SA	278	10.09	0.00	S
9	Use routine managerial activities as tools for supervision	3.18	3.26	3.25	SA	278	15.69	0.00	S
10	Use monitoring software to monitor performance	3.18	3.21	3.28	SA	278	2.96	0.05	NS
11	Use Google Alerts to generate updates of new action and to detect any harmful activity	3.13	3.21	3.32	SA	278	13.13	0.00	S
12	Use GFI LanGuard software to scan the network against vulnerabilities that are harmful to the institution's servers	3.13	3.23	2.28	SA	278	2.94	0.05	NS
13	Use Microsoft Message Analyzer to analyze network protocol traffics to monitor activities on the network	3.07	3.29	3.27	SA	278	14.39	0.00	S
14	Set up Microsoft Message Analyzer to assess multiple	3.18	3.19	3.16	SA	278	2.68	0.07	NS

	The Supervisory Regulatory Framework	Numbers of SMS = 82, TMS = 133, OMS = 177 Total Respondents = 392							
		$\overline{x}_{SMS}$	$\overline{x}_{TMS}$	$\overline{x}_{OMS}$	Rmk	Df	F-ratio	P-value	Rmk
	log data sources from a single pane								
15	Install Nagios to monitor institutions' critical systems, applications, and services	3.28	3.22	3.32	SA	278	1.49	0.23	NS
16	Set Nagios to generate alert whenever the systems are attacked	3.14	3.17	3.14	SA	278	6.99	0.00	S
17	Set Nagios software to generate reports on the system viability when attacked	2.14	3.06	3.09	SA	278	2.86	0.06	NS
18	Install OpenNMS to automate discovery of any intrusion	3.01	3.10	3.15	SA	278	3.13	0.05	NS
19	Use Capsa Free to monitor networks so as to detect if there is any intrusion	3.12	3.16	3.36	SA	278	3.65	0.03	S
20	Use MSN, Yahoo or Google Messenger to filter emails and customize reports when necessary.	3.09	3.22	3.33	SA	278	3.09	0.05	NS
	Grand mean	3.09	3.13	3.23	SA	278	0.88	0.42	NS

The result in Table 3 showed the mean ratings of respondents on the supervisory regulatory framework for effective information management in Public universities in South-South Nigeria. The result showed the mean ratings of the three group of respondents (Strategic, Tactical and Operational Management staff) to be greater than 3.0, implying that the 20 items are supervisory regulatory measures for effective information management in Public universities. moreover, the corresponding standard deviation to each of the items ranged from 0.38– 0.47 with an overall of 0.12, signifying that the opinions of the respondents were very close to one another.

The result in Table 3 further shows the ANOVA result of the hypothesis of no significant difference among the mean responses of Strategic, Tactical and Operational Management staff on supervisory regulatory measures adopted by them for effective information management in Public universities in South-South Nigeria. The result revealed a cluster F-value of 0.88 with a significant value (P-value) of 0.42. Since the overall P-value of 0.42 is greater than 0.05 set as level of significance, the null hypothesis (Ho2) was not rejected. Although the analysis revealed significant and non-significant p-values on different items, the hypothesis (Ho5) was not rejected because the overall p-value was not significant.

Based on the findings, the schematic representation of the conceptual regulatory framework of this study is depicted in Figure 1. Figure 1 depicts the relationships between the variables. Effective information management is the key player to the survival of Public universities particularly in today's information age. A close look at the schema reveals that effective information management involves establishment of internal regulatory measures such as information, communication, logical environment security and supervisory regulatory actions. Without good internal regulatory, it will be very hard if not impossible for public universities to achieve their goals and objectives. In previous years most institutions were keeping only offline documents, but recently technology has made it possible for these institutions to process, store, retrieve, and disseminate their information online thereby increasing the rate of information hack, intrusion, and sometimes complete loss of information/data to unauthorized web attacker. The implementation of information regulatory

measures will assist the management staff to deliver their functions effectively and by extension help their institutions to overcome all the threats and vulnerabilities to their information systems.
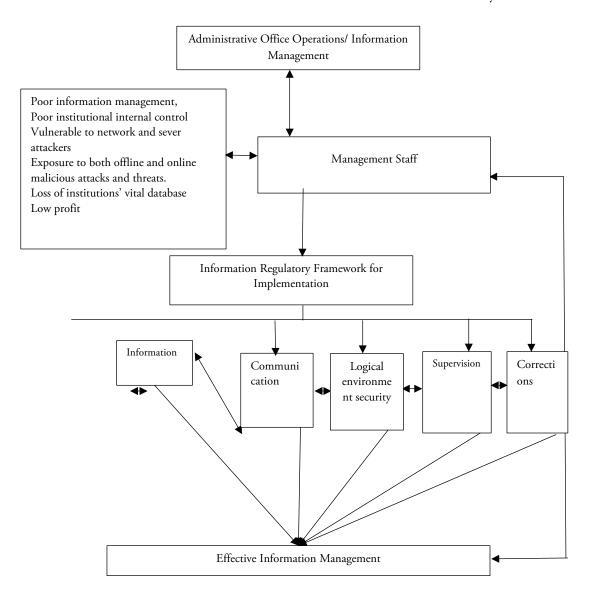

Figure 1: Regulatory Frameworks for Information Management. Source: The researchers (2022)

4.3. Discussion

The study revealed that the logical environment regulatory actions identified in this study are strongly needed by management staff in Public universities in for effective information management in Nigeria. Some of the logical environment regulatory actions identified include: demonstrate a commitment to integrity and ethical value by setting up standard of conducts; maintain the independence of the board of directors from management and their   oversight of the entity's internal regulatory; establish organizational structure, reporting lines, authority, and responsibilities to pursue institution's objectives; demonstrate a commitment to attract, develop, and maintain competent staff through constant trainings on information management; maintain accountability standard for the execution of internal regulatory responsibilities; specify appropriate objectives to support effective

environmental regulatory actions; identify and analyze risks, and evaluate fraud risks by checking the sources and causes of the risk as well as the weak points in the information systems.

These findings were congruent with Naboth-Odums et. al (2022) and Institute of Internal Auditors (20008) who noted that it is the responsibility of the board of directors and executive management of an institution to set the culture and attitude about the importance of maintaining logical regulations and also the standards of conduct within any organization. The findings of the study were also in line with Ibelegbu et. al. (2022), who asserted that it is part of the responsibilities of the strategic management team is to provide guidelines to subordinate staff. Hence, our regulatory framework on logical environment control actions is timely. The findings of this study again gave credence to the Tunji et. al. (2016) who observed that part of the logical environment include regular changes of dial-up numbers; use of dial-back access; use of software and hardware "firewalls" to restrict access to assets, computers, and networks by external persons; and regular changes of passwords and deactivation of former employees' passwords.

Our findings imply that management staffs in public universities in Nigeria strongly agreed to the supervisory regulatory actions, which when implanted, can drastically reduce information mismanagement in our Public universities. Also, our findings suggest that the level of the agreement by majority of the management staff on the supervisory regulatory measures for effective management of their institutional information is high. Some of the supervisory regulatory measures identified include: Monitor all the aspects of the institution's information centers that are most critical in fulfilling schools' long term goals; Specify a standard or range of satisfactory performance in service delivery; Know who, when, and how information about institution's data, file, transactions are to be collected and recorded; Specify the type of comparisons that will be made, and developing some possible responses if performance is outside the range; Identify the important stages of each information process; List the key inputs and outputs of each information process stage; Assign the right and capable staff to the supervisory unit, and Set special supervisory activities in high-risk information areas like financial, online transactions, identification code, and confidential documents.

The findings of this study strengthened National Vulnerability Database (2019) who noted that some of the reasons why organisations design and implement supervisory regulatory measures include: to attack or indicate potential attacks on institutions' information systems; ii) to identify unauthorized local network, and remote connections from malicious attacker. The findings are also in agreement with National Vulnerability Database (2019) who found that the information officers can maintain supervisory regulatory measures in an institution by strategically deploying supervisory devices to collect organization-determined essential information. The findings were also congruent with State of Vermont (2015) who found that supervisory regulatory are maintained through managerial activities such as supervision, reconciliations, checklists, comparisons, performance evaluations, and status reports. Furthermore, the findings of the study supported Chierotti (2014) who noted that management staff can use auto-discovering of devices on an institutions' network and reports back on their status to the appropriate office. Similarly, the findings of the study is in agreement with Fisher (2019) who maintained that one of the approaches to effective supervisory regulatory measures is by using OpenNMS to put surveillance over an institutions' databases and for automated discovery of any fraudulent attempt on the institutions' information system.

Although we have successfully presented viable regulatory frameworks on logical environment and supervisory control actions to ensure the sustenance of public institutions across the globe, however, some limitations were encountered in the process. Firstly, we engaged management staff in some selected Public universities in Nigeria. This posed a great deal of short comings on the generalization of our findings to other levels of tertiary institutions as well as othe related establishments across the globe. As a result, we suggest that a study of this kind be replicated in other level of teriary institutions and public agencies in Nigeria and elsewhere in order to determine if any significant difference would be observed in their findings using different methods and materials.

5. Conclusion

Our inferred that the identified 22 logical environment and 20 supervisory regulatory actions are frameworks for effective information management of public universities in Nigeria. The adoption of this framework has the tendencies to curb the plethora of high vulnerability the university's information systems to several online threats and malicious attacks. It is clearly established in this study that effective information management through the logical environment and supervisory regulatory actions are the keys to the survival of the institutions from the unscrupulous hackers. Diligent application of the identified regulatory actions will also help the management staff to check-mate against internal errors, frauds, and abuse of information by staff and students. Above all the statues, integrity and standard of the institutions will improve if the information regulatory actions are effectively implemented. It is therefore, imperative for the stakeholders of Public universities in Nigeria to take seriously the issues of adaptation of regulatory actions for effective information management of in the institutions.

We therefore recommended that Administrators and managements of Public universities in Nigeria should enact effective policies and laws that support the adaptation of procedural preventive regulatory actions in their institutions; management of Public universities should provide 21st-century ICT equipment that has updated applications that guarantee detective regulatory actions; Administrators and Heads of Information Departments should organize regular staff trainings to help and upskill the management staff on the effective application of Information and communication regulatory actions and the skills adopted for its effectiveness operation; management unit heads of the Public universities should organize trainings for the management staff on how to apply logical environment regulatory actions to guarantee an effective network of information security of the institutions; and since security is the responsibility for everyone, the Director of Academic Planning should organize trainings inform of conferences, seminars, symposiums and workshops for academic and teaching staff as well as students on the general information regulatory actions.

Acknowledgements

Conflict of Interest

The authors have no conflicting interests. The approval for this study was granted by the departments with whom the authors have affiliations with. Participants completed written informed consent form.

References

Abanyam, F. E., Ibelegbu, A. N., & Garba, H. J. (2020). Green marketing: The enviropreneur and compliance marketing approaches for predicting sustainable industries in Nigeria. Vocational and Technical Education journal, 4 (2), 265-277 www.acjol.org

Abanyamm, F. E. & Abanyam, V. A. (2021). Green Marketing in Nigeria Consumer Sustainability: The Distribution and Physical Practice on Polythene Manufacturing Companies. Journal of Contemporary Issues and Thought, 11(1), 126-140. https://doi.org/10.37134/jcit.vol11.11.2021

Abanyamm, F. E. & Guma, E. T. (2021). Utilization of Computer Assisted Instruction (CAI) for Effective Teaching and Learning of Financial Accounting in Senior Secondary Schools in Benue State, Nigeria. Asian Journal of Assessment in Teaching and Learning, 11 (1), 42-54. https://doi.org/10.37134/ajatel.vol11.2.5.2021

AbdulAzeez, A. T. (2016). Analysis of Management Practices in Lagos State Tertiary Institutions through Total Quality Management Structural Framework. Journal of Education and Practice, 7(8). Retrieved on June 7, 2019 from: www.iiste.org

Africa Cyber Security. (2016). African universities battle hacking, cybercrimes. Retrieved on May 4, 2019 from: https://punchng.com/african-universities-battle-hacking-cyber-crimes/

Chand, S. (2019). Decisions Making: Strategic, Tactical and Operational Decisions and Business Management. Retrieved on October 13, 2019 from: http://www.yourarticlelibrary.com/informationtechnology/decisions-making-strategic-tactical-and-operational-decisions-business-management/10271

Chierotti, J. (2014). Want to Keep Your Personal Information Private? Monitor Your Online Reputation! Retrieved on September 12, 2019 from: https://www.socialmediatoday.com/content/want-keep-your-personal-information-private-monitor-your-online-reputation

Ewepu, G. (2016). Nigeria loses N127bn annually to cyber-crime. NSA. Retrieved from http://www.vanguardngr.com/2016/04/nigeria-loses-n127bn-annually-cyber-crime-nsa/

Fabunmi, M. (2006). Perspective in educational planning. Ibadan: Odun Printers and Pack

François, M. T. (2016). A quantitative study on the relationship of information security policy awareness, enforcement, and maintenance to information security program effectiveness. An Unpublished Dissertation Presented in Partial Fulfillment of the Requirements for the Degree Doctor of Philosophy to School of Business and Technology, Capella University.

Gauthier, R. (2014). Major event legislation: Lessons from London and looking forward. The International Sports Journal, 14(1-2), 58-71. http://dx.doi.org/10.1007/s40318-013-0034-0

Ibelegbu, A. N. & Abanyam, F. E. (2022). Human Resource Management: Impact of Employees' Relations and Training Practices of Listed Deposit Money Banks' (LDMB) Performance in Adamawa State, Nigeria. Journal of Business Strategy Finance and Management, 4(1). Available From: https://bit.ly/3qDq0ow

Janssen, D., & Janssen, C. (2019). Electronic data interchange. Technopedia. Retrieved on September 8, 2019 from: https://www.techopedia.com/definition/1496/electronic-data-interchange-edi

Johnson, M. (2009) What are business operations? Retrieved on November 11, 2019. From: https://resources.work.com/management-officer-job-description

Jumper, J. P (2005). Levels of air force leadership. Retrieved on November 16, 2019 from: https://www.doctrine.af.mil/Portals/61/documents/Volume_2/V2-D10-Levels-Leadership.pdf

Kenneth C. Laudon, K. C., & Laudon, J. P. (2014). Management Information Systems: Managing the Digital Firm, (13th Ed). USA: Pearson. Retrieved on September 8, 2019 from: https://www.pearson.com/us/higher-education/product/Laudon-Management-Information-Systems-Managing-the-Digital-Firm-13th-Edition/9780133050691.html

Martin, R. (2011). The three levels of leadership. Retrieved on November 16, 2019 from: https://exploitingchange.com/2011/02/28/the-three-levels-of-leadership/

Mattie, J. A., Hanley, P. F., & Cassidy, D. L. (2005). Internal regulations: The key to accountability. Retrieved on November 21, 2019 from: www.ucop.edu/riskmgt/erm/documents/pwc_int_ctrls.pdf

McCrindell, J. Q. (2015), Framework for financial management and regulatory. Journal of Finance Management Institute, 16(2) pp, 11-39

Mellon, B. (2013). US research universities increasingly targeted by cyberattacks. Retrieved on May 3, 2019 from: http://www.upi.com/Top_News/US/2013/07/17/US-research-universities-increasingly-targeted-bycyberattacks/26641374065244/

Mendez, R. (2015). General regulatory vs. application regulatory. Prezi. Retrieved on September 8, 2019 from: https://prezi.com/iacknmfi6oxg/general-regulatory-vs-application-regulatory/

Mikoluk, K. (2013). Planning in management: strategic, tactical, and operational plans. Retrieved on October 13, 2019 from: https://blog.udemy.com/planning-in-management/

Misra, G. (2019). Office Operations: Meaning, Importance and Classification. Retrieved on May 31, 2019 from: http://www.yourarticlelibrary.com/office-management/office-operations-meaning-importance-and-classification/74657 .

Naboth-Odum, A., Abanyam, F. E., Abdulkadir, A., & Abanyam, V. A. (2022). Information and Security Control Mechanisms Embraced for Effective Information Management in Colleges of Education in Nigeria. Golden Ratio of Social Science and Education, 2 (2), 98-111. https://doi.org/10.52970/grsse.v2i2.183

National Vulnerability Database (2019). Security and privacy regulations for federal information systems and organizations. Available at https://nvd.nist.gov/800-53/Rev4/regulatory/SI-4

Neelameghan, A.. (2008). Information systems for national development - the social relevance of information systems. International Forum on Information and Documentation, 5 (4), 3-8.

Okolo, N. B. (2015). Evaluating factors of security policy on information security effectiveness in developing nations: A case study of Nigeria. An Unpublished Dissertation. Presented in Partial Fulfillment of the Requirements for the Degree of Doctor of School of Business and Technology Management, Prescott Valley, Arizona.

Osuala, E. C. & Okeke, A. U. (2006). Management office management. Enugu: Cheston Agency Ltd.

Rogers, G. & Ashford, T. (2015). Mitigating higher ed cyber-attacks. ASCUE Proceedings, 5(2), 234-241.

Rouse, M. (2014). Electronic data interchange. Retrieved on September 8, 2019 from: https://searchdatacenter.techtarget.com/definition/EDI

State of New York Comptroller, (2007). Standards for internal regulatory in New York State government. Retrieved on November 21, 2019 from: https://osc.state.ny.us/agencies/ ictf/docs/intregulatory_stds.pdf.

State of Vermont, (2015). Supervisory, assessment and planning. Retrieved on November 20, 2019 from: https://dec.vermont.gov/watershed/map

The Institute of Internal Auditors, (2008). Practice guide: Auditing the regulatory environment. Retrieved on September 11, 2019 from: https://na.theiia.org/standards-guidance/recommended-guidance/practice-guides/Pages/Auditing-the-Regulatory-Environment-Practice-Guide.aspx

Tunji, O., & Nelson, O. (2011). The effect of e-portal system on corporate image of universities. i-manager's Journal of Educational Technology, 7 (4), 345-349.

Wynn, C. L. (2017). Examining the relationship of business operations and the information security culture in the united states. An Unpublished Dissertation. Presented in Partial Fulfillment of the Requirements for the Degree of Doctor of Computer Science to Colorado Technical University.