Asia-Pacific Journal of Educational Management Research
Vol. 7, No. 1 (2022), pp. 1-20
http://dx.doi.org/10.21742/ajemr.2022.7.1.01

Procedural Preventive and Detective Control Measures Adopted by Administrative Officers for Effective Information Management in Colleges of Education in South-South, Nigeria

Augustine Naboth-Odums[1], Friday Ekahe Abanyam[2*], Nathaniel Ifeanyi Edeh[3] and Abdulrahman Abdulkadir[4]

[1]*School of Business Education, Federal College of Education (Technical) Omoku, River State, Nigeria*
[2*]*Department of Business Education, Faculty of Education, Ambross Alli University, Ekpoma, Edo State, Nigeria*
[3]*Department of Business Education, Faculty of Vocational and Technical Education, University of Nigeria, Nsukka, Nigeria*
[4]*School of Business Education, Federal College of Education (Technical) Gombe, Gombe State, Nigeria*
[1]*naboth-odumsaustin@gmail.com,* [2*]*fabanyam@aauekpoma.edu.ng,*
[3]*ifeanyi.edeh@unn.edu.ng,* [4]*balaab@fcegombe.edu.ng*

Abstract

Cybercrimes and hacking activities have hindered the smooth management of several tertiary institutions. This has been attributed to poor information control measures. Based on this background, it is very salient that school management put in place good information control measures to safeguard their institutions from unforeseen hacks and cyber-attacks. Hence, the present study determined the procedural preventive and Detective control measures adopted by administrative officers for effective information management in Colleges of Education in South-South Nigeria. The study adopted a descriptive survey research design. The population for the study was 1580 consisting of 232 Strategic, 569 Tactical, and 779 Operational Administrative Officers from the 11 colleges of Education across the six states that make up South-South Nigeria. 320 respondents using a proportional sampling technique were used to determine the number of the strategic, tactical, and operational administrative officers for each of the colleges of education studied. The instrument for data collection was a structured questionnaire titled "Information Management Control Measures Questionnaire (IMCMQ)" which was developed by the researcher in line with the reviewed literature. The questionnaire was face-validated by five experts. The reliability of the instrument was tested using the Cronbach Alpha method to determine its internal consistency and this yielded an overall coefficient of 0.93. Mean, standard deviation, and Analysis of Variance were used to analyze the data collected. The findings showed that the administrative officers highly adopted procedural preventive control but moderately adopted the identified detective control measures for effective information management. The findings of the hypotheses t showed that there was no significant difference among the opinions of the respondents on the level at which they adopt the procedural preventive and detective control measures for effective information management of their

Article history:
Received (January 27, 2022), Review Result (February 28, 2022), Accepted (April 14, 2022)

Print ISSN: 2207-5380, eISSN: 2207-290X AJEMR

institutions. Based on the findings, it was recommended among others, that the management of colleges of education in Nigeria should enact and implement effective policies and laws that support the adoption of information control measures for effective information management in their institutions.

Keywords: *Procedural preventive control, Detective control measures, Administrative officers, Effective information management, Colleges of education*

1. Introduction

Colleges of Education (COEs) are among the tertiary institutions in Nigeria that were established by the Act of Parliament to cater for the training of middle-level manpower in the teaching profession. COEs award the Nigeria Certificate in Education (NCE) as the minimum teaching certificate and qualification for Nigerian teachers. The products of these institutions are groomed to teach at the Pre-Primary, Primary, and junior secondary school levels and/or proceed to university education. College of Education programs are run for three years including four months Student Industrial Work Experience Scheme and six months of teaching practice [1]. The author posited that the NCE program was introduced to prepare individuals to become leaders and practitioners in education and in related human service fields by expanding and deepening their understanding of education as a fundamental human right.

Currently, there are one hundred and fifty-two approved COEs in Nigeria, made up of twenty-one Federal COEs, forty-nine State Government-owned colleges, and eighty-two privately owned COEs [1]. The chief executive of a College of Education in Nigeria is designated as Provost while the head of administrative office operations is called the Registrar, with the Deputy Provost, Bursar, and College librarian as the principal Officers. The collective decision of these principal officers and the Deans of Schools (faculties) is often referred to as "management decisions". To take the right decisions for the effective administration of any college, the management needs the right information at the right time and in the right form, which is usually processed by the Administrative officers in various administrative offices in colleges.

Administrative offices serve as support units to all other departments in COEs in Nigeria. The administrative office, according to Agomuo [2], is a place where clerical functions necessary for information handling are carried out. Similarly, Osuala and Okeke [3] posited that an administrative office is a place in which administrative operations such as record keeping, information processing, consultation, and other kinds of clerical activities are performed. To enable COEs to provide qualitative education, research, and community services, administrative office management is needed for information creation, processing, and disseminating, which is the key function of the office. The dissemination of information could be in form of providing information on admission of students, making periodic reports on academic matters, information on students' accommodation, issues of school fees and registration, and information on security and human resource matters.

Administrative office operations are concerned with the coordination of finance, and operational performance of routine office tasks [5]. This involves handling information appropriately on daily basis. According to Abanyam and Guma [6], information is a corporate resource and it is what office operations produce. The author further stressed that all office workers are information workers while administrative officers are information officers. In any administrative office, operations such as receiving information, processing information,

storing information, disseminating information, and recovering information are handled by the Administrative Officers (AOs).

Administrative officers in COEs deal 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 concerning fiscal and other matters. According to Meyer [7], administrative officers are the greatest resource of COEs because they make a 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 COEs must be beneficial to the way administrative officers manage information. According to National Commission for Colleges of Education [1], there are seven cadres of administrative officers in COEs, namely: Deputy Registrar, Principal Assistant Registrar, Senior Assistant Registrar, Assistant Registrar, Administrative Officer I, and Administrative Officer II.

However, in management, there are three major classifications of managerial levels, namely: strategic, tactical, and operational levels [8][9][10]. This classification is based on the functions and responsibilities of the administrative officers. According to Osuala et. al. [3], the levels of management are traditionally represented as strategic, tactical, and operational. The authors added that the strategic managers are referred to as the top-level managers. The tactical managers are the middle-level managers, while the operational managers are the low-level managers. The strategic managers are concerned with the planning functions of an organization, policy formation, and the development of the 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 main function of the tactical managers is centered on organizing, coordinating, and staffing while the operational managers are the supervisors. They direct, control, and monitor workers to perform the planned activities. They check workers' attendance, maintain quality control, handle complaints, track schedules, and costs, and ensure effective and efficient maximization of workers' input to duty [10]. The degree of success of any educational institution depends on the extent to which the administrative officers can manage the information systems.

Information management (IM) concerns a cycle of organizational activity: the acquisition of information from one or more sources, the custodianship and the distribution of such information to those who need it, and its ultimate disposition through archiving or deletion. According to the State of Vermont [11], for an institution to run and control its operations effectively, it must have relevant, valid, reliable, and timely information relating to internal and external events. Administrative officers must be able to provide reliable information to enable management to make informed decisions, determine their risks, and communicate policies and other important information to those who require it. State of Vermont [11] concluded that information management encompasses all the generic concepts of management including planning, organizing, structuring, processing, evaluation, and reporting of information activities, all of which must be controlled administratively. Operationally, information management is the acquisition, processing, storing, distributing, and providing of information when necessary for the effectiveness of information systems in COEs with the sole aim of achieving the institutions' set goals. Effective information management involves the application of administrative control measures to ensure that information is properly processed, secured, and delivered as when due.

Administrative control is a critical function of management. According to the State of Mississippi Department of Finance and Administration [12], administrative control comprises policies, plans, procedures, and practices used to manage the organization and meet the

organizations' goals and objectives. Administrative controls are concerned with directing the activities of others, to ensure that office workers do what is expected of them. They serve as means of managing the risks associated with programs and operations. According to Lucey, [12], control encompasses procedures designed to provide reasonable assurance regarding the achievement of effectiveness and efficiency of operations, reliability, and integrity of information, and compliance with applicable laws and regulations in the management of the organization. In this study, administrative control is the process of ensuring that actual activities of the COEs concerning information management conform to established standards and laid down procedures. These standards are contained in the Acts that established COEs in Nigeria, in the minimum standard (Benchmark), in the Curriculum framework, and also in the Conditions and Schemes of Service for COEs in Nigeria.

The control helps the college management to monitor the effectiveness of information staff. Administrative controls are concerned with directing the activities of others, to ensure that office workers do what is expected of them. One of the main objectives and strengths of an effective control measure as pointed out by Osuala et al. [13] is to enhance the ability of administrators to manage, release their management potentials, and act as a positive force for achieving the aims and objectives of the information system in the organization. Administrative officers in COEs require adequate control measures for information management to be able to provide the needed information for effective decision-making. Such control measures help to make administrative officers accountable for their actions but should not be regarded as a constraint to their freedom to make decisions in areas for which they have authority.

Several administrative controls can be adopted by educational institutions in Nigeria, but the depth with which they operate may vary according to the peculiarity of the institution. Administrative controls are classified as procedural preventive and detective measures [14]; logical security and environmental control measures [15]; storage, information communication, environment (physical), and monitoring measures [16][17]; and recovery control measures [18][19]. In this study, however, procedural preventive and detective controls shall be of interest to the researchers.

Procedural preventive controls (or work practice controls) are typically in the form of standard operating procedures that define how certain types of information are to be handled, or how specific operations are to be conducted. Procedural preventives controls are part of the control activities which set forth the fundamental framework and the underlying methods and procedures that employees rely upon to do their jobs. Procedural preventive control measures, according to Lucey [12], are designed to avoid errors or improprieties before data is processed. These measures provide specific direction and help form the basis for which decisions are made every day by employees. Within the organizational structure, management must clearly and adequately: define areas of authority and responsibility; appropriately delegate the authority and responsibility throughout the information management departments; establish a suitable hierarchy for reporting; support appropriate human capital policies for hiring, training, evaluating, counseling, advancing, compensating and disciplining personnel; and uphold the need for personnel to possess and maintain the proper knowledge and skills to perform their assigned duties as well as understand the importance of maintaining effective internal control within the organization. Without this framework of understanding by employees, conflict or inconsistencies can occur, poor decisions can be made and serious harm can be done to the department's reputation [15]. Furthermore, the efficiency and effectiveness of operations can be adversely affected. The effectiveness and efficiency of operations such as information management help to ensure that inherent dangers

and threats are detected early enough to avoid losses. This can also be achieved through detective control measures.

Detective control measures (also known as back-end control activities) are designed to identify errors or irregularities that have already occurred and enable management to take prompt corrective action. Examples of detective controls are editing of reports and emails, reconciliations, management reviews, audits, financial and budgetary reviews, and analysis. Gauthier [16] observed that these control measures can be manual or automated. Manual control activities are performed by individuals, such as preparing a bank deposit or performing reconciliation, recording, and calculation of students' result scores and result computation [17][18]. Automated controls are incorporated into application systems. Automated controls are considered more reliable, due to their ability to prevent errors from being entered into the system (e.g., inaccurate vendor identification) and by detecting/correcting errors within the system (e.g., exception reports). Additionally, automated controls occur consistently with every transaction, whereas manual controls are more susceptible to human error [19]. IT-dependent manual control activities are manually performed but require an input based on the results of computer-produced information. Management relies on the information system to identify variances and produce the variance report for effective managerial decision-making. Such reports and other information assets can be secure using logical security control.

For better performance of administrative duties, administrative officers in COEs must ensure that the institution's information and resources are used efficiently and effectively to achieve desired objectives. Information and resources must be used consistently with the missions of the institution in compliance with laws and regulations, and with minimal waste of resources, fraud, and mismanagement. It is very necessary to emphasize that it is the responsibility of the institutions' information managers to develop and maintain effective control measures over the institutions' information systems. The demand for effective information security measures 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. According to Mellon [20], there are about 90,000 to 100,000 cyber attempts and attacks per day on institutions' websites. The author lamented that such attacks have resulted in a lot of data breaches of several staff and students. In Nigeria, several such attacks have been observed. According to Egwu [21], as of 2016, Nigeria is ranked 16th highest country in cyber-attack vulnerabilities in Africa. Several tertiary institutions have suffered a cyberattack in Africa including Nigeria. According to a report by Africa Cyber Security [22], African countries have lost about US$2 billion in cyberattacks in 2016 only. Similarly, researchers have found that there are several cases of cybercrimes and fraudulent activities against tertiary institutions' websites, digital documents, databases, and networks in Nigeria and particularly in the study area [23]. 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 control measures, and failure to patch and secure institutional information systems. Based on this background, it is very salient that the management of COEs in Nigeria put in place good information control measures to safeguard their institutions from unforeseen hacks and cyberattacks. It is against this background that the present study sets to determine the detective control measures adopted by administrative officers for effective information management in COEs in South-South Nigeria.

1.1. Research questions

The following research questions guided the study:

1. What are the procedural preventive control measures adopted by administrative officers for effective information management?
2. What are the detective control measures adopted by administrative officers for effective information management?

1.2. Hypotheses

The following null hypotheses formulated to guide the study were tested at a 0.05 level of significance:

1. There is no significant difference in the mean responses of strategic, tactical, and operational administrative officers on the procedural preventive control measures adopted for effective information management.
2. There is no significant difference in the mean responses of strategic, tactical, and operational administrative officers on the detective control measures adopted for effective information management.

2. Literature review

2.1. Administrative office operations

It is necessary to state here that there are three levels of hierarchical classification at the administrative level, namely: Strategic, tactical, and operational levels. This classification helps to define the functions and duties of the administrative officers.at the strategic level, plans are designed with the entire organization in mind and begin with an organization's mission [24]. The author opined that top-level managers, such as Chief Executives Officers, Presidents, Provost, Vice-Chancellors, Directors, Faculty Deans, and Principal officers, among others design and execute strategic plans and set up policies, thus, establishing a framework of operation for the desired future and long-term goals of the organization. Essentially, strategic plans look ahead to where the organization wants to be in three, five, or even ten years. Strategic plans, provided by top-level managers, serve as the framework for lower-level planning. Mikoluk [10] noted that tactical plans support strategic plans by translating them into specific plans relevant to a distinct area of the organization. Tactical plans are concerned with the responsibility and functionality of lower-level departments to fulfill their parts of the strategic plan. These are the major functions of the middle-level manager. Examples of staff under tactical levels in institutions of learning are Deans, Directors, and Senior Managers, among others. Operational plans are at the bottom of the management pole; they are the plans that are made by frontline, or low-level, managers. All operational plans are focused on the specific procedures and processes that occur within the lowest levels of the organization [10].

Managers must plan the routine tasks of the department using a high level of detail. At the operational level, the lower-level managers carry out the planned activities designed by the middle-level managers into achievable goals. Staff under operational levels include Heads of Departments, Deputy Registrar, Administrative Officers (Principal Assistant Registrar, Senior

Assistant Registrar, Assistant Registrar, etc. For this study, the administrative officers in COEs are grouped into three, namely: strategic group, tactical group, and operational group. The administrative officers under the strategic group include Deans of schools, the college bursar, Libertarian, directors, and the Registrar; and for the tactical group, we have Deputy Registrars, principal assistant registrars, senior assistant registrars; and finally, under the operational group, we have assistant registrars, administrative officers I, and administrative officers II shown in Figure 1.

Figure 1. Managerial (Information Managers) levels in an organization

2.2. Information management in higher educational institutions

Effective information management has placed a demand on administrative office operation/management because of institutional management's demand for properly processed and organized information. For institutions to survive the challenges of the modern technology competitions in the world of industries and business, information must be presented in the form needed for accurate and more effective management decision makings. Authors stressed that in the dynamic world of industry, business, and education, information management is never static but always changing in the interests of greater efficiency [25][26]. This implies that for the administrative office operation of any institution to succeed, reliable and adequate administrative control measures must be put into place. Devising better ways of managing information is very important in COEs because of the level of sophistication of information processing demanded by the day-to-day business challenges of modern-day education and the technologies involved. Hence, Abanyam [27] argued that the concept of information management is just timely and a response to the growing demand for better handling of information in the face of the rapidly growing world of education and industry.

Importantly, some information communication experts and educationists have argued that the use of online portals can promote the overall corporate image of educational institutions across the world [28]. Authors have opined that the corporate image of an institution determines how the public and stakeholders perceive such institutions and this is often showing how well such institution is doing in terms of delivering its objectives and meeting up with its mandates [29]. This has increased the attention of institutional administrators on the roles of the administrative offices.

2.3. Procedural preventive control measure

A procedure is an established, organized, or routine method set for doing something. Procedural preventive control measure is an organized method established by an institution to help proactively prevent or stop undesirable harm from happening. Lucey [12] defined procedural preventive control measures as organized and routine information designs established by an institution to check and prevent information mismanagement, unauthorized access, and modalities of recovering lost information. The author maintained that properly designed procedural preventive control measures help an institution evade errors or improprieties of information ahead of time before risk or harm occurs. The measures provide a distinctive direction through which information management can flow such that missing data can be traced. The system also helps in forming the basis upon which management decisions can be based.

Bradford [30] postulated that procedural preventive control measures prevent theft, fraud, misstatements, and ineffective organizational or institutional functioning. Bradford argued that one of the best practices of implementing an effective procedural preventive control is by setting up a segregation of duties and staff roles. This control can also be done by using locks and access codes on sensitive administrative offices or using passwords to encrypt confidential data and information.

National Vulnerability [31] postulated that procedural preventive control measures are purposefully designed by organizations merely to deter errors, irregularities, and fraudulent activities from occurring in information management. The author maintained that procedural preventive control measures are proactive controls that help to ensure that institutional objectives are being met. It is typically in the form of standard operating procedures which define how some institutional information is managed, or how specific operations are carried out. Authors are of a similar view that procedural preventives control measures are part of the fundamental framework of control activities, methods, and procedures set forth by the administrative staff of an institution as internal control systems which guide employees while they carry out their daily jobs [16][30][32].

According to Misra [33], wireless communication standards usually provide several security protocols for local wireless connections. These kinds of networks were formally protected using the Wired Equivalent Privacy (WEP). However, researchers have shown that WEP has proven insecure in protecting information or communication on the wireless network [34]. Unfortunately, many institutions still use WEP to secure their information even when it does not support or protect wireless communication. In line with this, it is believed that wireless networks are common in organizations and individuals' networks. However, this wireless networking has several security issues.

2.4. Detective control measures

Detective control measures also called back-end control activities are designed to detect or identify frauds, omissions, errors, or irregularities that have already occurred, thus allowing management to take immediate corrective action. According to the University of California [35], detective controls measures to attempt to detect undesirable acts. The author noted that the system provides evidence that a loss occurred but it does not prevent a loss from occurring. According to Thomas et. al. [36], detective controls measures are management information control tools that are designed to spot undesirable activities so that corrective actions can be taken. The authors argued that detective measures are implemented to assist in detecting malicious activities by unauthorized and unscrupulous persons. Thomas et. al. [37]

noted that though detective controls do not stop intrusion attempts by attackers, it identifies and reports that such activity took place so that management can take appropriate measures and actions to mitigate the attempt. Other detective measures that can be employed are by using an access log and alert system which can quickly detect fraud and notify management of any attempts by employees or unauthorized users to access institutions' information or parts of an information room or building [38].

Furthermore, management can also use other detective measures such as reconciliations, management reviews, audits, financial and budgetary reviews, and analysis to spot unauthorized activities' Gauthier [16] pointed out that these detective control measures can be applied in manual or automated manners. Manual control activities involve using individuals i.e. workers who will carry out the activities. Take for instance a worker who is assigned to make a bank deposit or do a reconciliation of account. On the other hand, in automated control measures, application systems are incorporated into information systems. The function of the application is to help to detect any fraud attempt and to report to management using signals or alarms depending on the setting given to it. Several authors are of the view that automated control measures are more reliable than manual control. This is because of the ability of the application or detective software to prevent errors from intruding into the system and helps in detecting/correcting errors within the system.

Bradford [30] asserts that detective control concerning security over digital documents is mainly designed to detect attacks targeted at institutions' information systems and prevent such from being successful. The author maintained that the detective controls are designed to find out system or hardware faults and provide warnings or signals to information officers or system administrators to prevent system interruptions. Thomas et al. [37] and Abanyam and Abanyam [39] observed that detective security software was developed by security vendors and software companies develop to enable institutions to protect their networks and online data. They include firewalls, intrusion detection systems, and honeypots. Cooper [40] stated that an intrusion detection system monitors network traffics for unusual or suspicious activities and consequently sends an alert to the information administrator. One of the ways IDS uses to detect malicious attacks is by matching an identified behavior to known signatures. This approach is referred to as signature-based intrusion detection (SID). Further to firewall and intrusion detection systems, organizations can also detect threats on their connections and networks using honeypot. If attackers found that the system is entrapment or decoy, they will ignore the honeypot and seek other points of weakness to attack.

3. Methodology

3.1. Design of the study

This study adopted a descriptive survey research design. A 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 items considered to be representatives of the entire group [6]. This design is therefore considered suitable for this study because it makes use of a questionnaire to collect data from the respondents on control measures adopted by administrative officers for effective information management in COEs in South-South Nigeria.

The rationale for adopting this method boils down to the fact that, though, a relatively small stretch of land, the South-South provides the economic mainstay of Nigeria, which is oil. In addition to oil and gas, the region equally contributes other key resources such as Tourism and Agriculture. The researcher's interest in South-South Nigeria is further based on

the turbulent nature of the zone to the hacking of information. There have been several reports of cybercrimes and hacking activities against educational institutions' databases and networks in the area [46]. Most tertiary institutions in the area express that they witness various breaches of information, however, they hardly identify when the attack is attempted until much later when it has done serious harm to the institutions.

3.2. Population and sample for the study

The population for the study was 1,580 consisting of 232 strategic, 569 tactical, and 779 operational administrative officers from the 11 COEs across the six states that make up South-South Nigeria. The strategic, tactical, and operational administrative officers were chosen because they are the main information management staff of the COEs. Again, they possess the experience and expertise required for effective information management therefore, were in a good position to respond to questions about the administrative information on control measures adopted for effective administrative office operations in the Colleges.

The sample size of the study was 320 respondents from the 11 COEs across the six states that make up South-South Nigeria. Taro Yamene's formula in Abanyam [27] was used to determine the sample size of the respondents from the COEs being studied. After determining the sample size, a proportionate sampling technique was used to determine the number of the strategic, tactical, and operational administrative officers for each of the COEs studied

3.3. Instrument for data collection

The instrument used for data collection was a structured questionnaire titled "Information management Control Measures Questionnaire (IMCMQ)" developed by the researcher. The questionnaire sought information on the procedural preventive control measures and detective control measures adopted by administrative officers for effective information management in COEs with 25 and 22 items respectively and was structured on a 4-point scale with response options of Very Highly Adopted (VHA), Highly Adopted (HA), Moderately Adopted (MA), and Lowly Adopted (LA) with weights of 4, 3, 2, and 1 respectively.

The questionnaire was face-validated by five experts. The questionnaire was trial-tested on a sample of 30 administrative officers in Alvan Ikoku Federal College of Education Owerri, Imo State, Nigeria, which is outside the study area. Cronbach Alpha reliability method was used to determine the internal consistency of the instrument which yielded 0.83 for procedural preventive and 0.97 for detective control measures with an overall coefficient of 0.93.

3.4. Method of data collection and analysis

The researcher with the help of eleven (11) research assistants, one for each of the 11 Federal and State COEs in the South-South administered the questionnaire to the respondents. The researchers found it challenging to obtain responses from some of the strategic administrative officers who rightly decline the request to provide information for this research, despite repeated attempts and persuasion. Also, many respondents were persuaded to participate in the study because they had no interest in answering the questionnaire and allowing themselves to be used for the study. While the participants were willing to be involved in the study, some of them complained about a large number of questionnaire items. These discouraged them from responding to the questionnaire. The apathy to responding to the questionnaire by some respondents as well as the inability of the researcher to obtain

qualitative information from the respondents would affect the efficacy of the generalization and validity of the study. However, the researchers partially dealt with these situations by pacifying some of the participants with incentives, which motivated them to comply accordingly. Therefore, three hundred and twenty (320) copies of the questionnaires were administered to the respondents while two hundred and eighty (280) representing an 87.5% rate of returns of correctly completed questionnaires were retrieved after two (2) weeks from respondents and were used for the data analysis (i.e. S=45, T=96, O=139 respectively).

Data analysis was done using mean, standard deviation, and Analysis of Variance (ANOVA). The real limit of numbers was used for interpreting the analyzed data as shown in [Table 1].

Table 1. Real limit of numbers for interpreting the analyzed data

Serial number (S/n)	Response Categories	Values	Point Boundary Limit
1	Very Highly Adopted (VHA)	4	3.0 – 4.0
2	Highly Adopted (HA)	3	2.0 – 2.9
3	Moderately Adopted (MA)	2	1.0 – 1.9
4	Lowly Adopted (LA)	1	0.0 – 0.9

In the test of hypotheses, the hypothesis of no significant difference was not rejected if the probability value is greater than or equal to a 0.05 level of significance. However, where the probability value is less than 0.05 level of significance, the null hypothesis was rejected. The Analysis of Variance (ANOVA) was used to test the hypotheses because the study compares the mean responses of three groups, namely: Strategic administrative officers, tactical administrative officers, and operational administrative officers.

4. Result

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. Research question/hypothesis one

Table 2. ANOVA of the Mean responses of administrative officers on the procedural preventive control measures adopted by them for effective information management

S/no	The procedural preventive control measures	Nos of S = 45, T = 96, O = 139. Total Respondents = 280							
		$\bar{x}_S$	$\bar{x}_T$	$\bar{x}_O$	Rrks	Df	F-ratio	P-value	Rmk
1	Put policies that support securing information assets such as hardware, software, and digital and non-digital resources of the institutions.	2.31	2.34	2.34	HA	319	0.00	1.00	NS
2	Put guiding rules that support restricting unauthorized access to ICT equipment, inventories, and other information assets.	1.41	1.35	1.33	MA	319	0.48	0.62	NS
3	Mount strong physical securities in all aspects of the information system.	2.45	2.5	2.38	HA	319	5.46	0.01	S
4	Put surveillance and restrict access to confidential places where confidential documents are housed.	3.35	3.18	3.27	HA	319	2.68	0.07	NS
5	Assign information officers on a	3.24	3.14	3.26	HA	319	2.47	0.09	NS

	routine basis to check through information assets and compared them to the value shown on control records.								
6	Use segregation of staff duties as a preventive control measure to protect institutional assets and resources.	2.27	2.18	2.36	HA	319	5.95	0.00	S
7	Use separation of duties as a measure to limit the amount of power and influence held by a particular individual in an office.	2.29	2.14	2.31	HA	319	5.49	0.01	S
8	Use separation of duties to prevent any form of 34conflict of interest, abuse, errors, and fraudulent acts.	2.33	2.18	2.35	HA	319	4.61	0.01	S
9	Ensure that the financial officer receiving cheques is not the person approving write-offs, depositing cash and bank reconciling statements, and keeping checkbooks.	3.57	3.22	3.33	HA	319	9.30	0.00	S
10	Specify policies for appropriate delegation of authority, and a clear hierarchy for reporting.	3.47	3.17	3.45	HA	319	12.90	0.00	S
11	Enact policies that support hiring, training, appraisal, placement, and rewarding of personnel that distinguished themselves in integrity and security consciousness.	3.41	3.18	3.39	HA	319	4.33	0.01	S
12	Ensure that no single staff has complete or absolute control over the information system environment.	3.35	3.33	3.32	HA	319	3.21	0.04	S
13	Use security protocols to prevent unauthorized access to institutional digital information resources.	2.43	2.27	2.29	HA	319	2.16	0.12	NS
14	Wi-Fi Protected Access protect their networks as well as their online information.	2.33	2.24	2.34	HA	319	1.96	0.14	NS
15	Wi-Fi Protected Access 2 to secure PCs and laptops connected to a Wi-Fi network.	2.55	2.67	2.75	HA	319	0.30	0.74	NS
16	Use Concurrent Security Standards to protect PCs and laptops connected to some older network cards.	1.32	1.43	1.47	MA	319	5.62	0.00	S
17	Use Secure Socket Layer to protect information systems, internet communications, and online transactions.	1.31	1.27	1.35	MA	319	2.15	0.12	NS
18	Use Transport layer security (TLS) to protect and prevent spying, tampering, message forgery, and internet threat and attacks.	1.41	1.23	1.29	MA	319	15.65	0.00	S
19	Use TLS to protect instructional Web browsers, e-mail, instant messaging, and all forms of voice over the Internet.	1.35	1.31	1.06	MA	319	12.60	0.00	S
20	Use TLS to secure all online communications between institutions' Web servers and browsers.	1.35	1.16	1.32	MA	319	4.17	0.02	S
21	Configure File Transfer Protocols (FTP) for effective and secured transfer of data	1.24	1.08	1.22	MA	319	3.85	0.02	S

	online.								
22	Use FTP to secure mailing files to workers, students, and stakeholders of the institutions.	1.27	1.31	1.16	MA	319	5.99	0.00	S
23	Use FTP to protect organizational data against unauthorized access and threat.	1.29	1.41	1.32	MA	319	7.26	0.00	S
24	Configure client-server with FTP to support file transfers and sharing through a remote computer.	1.33	1.34	1.21	MA	319	2.92	0.06	NS
25	Secure online transactions, and digital documents with supporting institutional ICT policies and laws.	2.37	2.35	2.31	HA	319	8.20	0.00	S
	Grand mean	2.20	2.12	2.17	HA	319	0.98	0.38	NS

Key: xS = Means of Strategic Administrative Officers, xT = Means of Tactical Administrative Officers, xO = Means of Operational Administrative Officers, S = Strategic Administrative Officers, T = Tactical Administrative Officers, O = Operational Administrative Officers, Rmk = Remark, NS = Not Significant, S = Significant. HA= Highly Adopted, MA = Moderately Adopted; LA = Lowly Adopted

The result presented in [Table 2] showed that items 1, 3-,6, 9-15, and 25 had mean values ranging from 2.25 to 3.35 indicating that these measures are highly adopted, while Items 2, 16 – 24 with mean of 1.18 to 1.35 showed that they are moderately adopted. The corresponding standard deviation for each of the items ranged from 0.38 – 0.49 with an overall of 0.45, signifying that the opinions of the respondents were very close to each other.

[Table 2] further showed the ANOVA result of the hypothesis of no significant difference among the mean responses of strategic, tactical, and operational administrative officers on procedural preventive control measures adopted by them for effective information management in COEs in South-South Nigeria. The result revealed an overall F-value of 0.98 with a significant value (P-value) of 0.38. Since the significant value of 0.38 was greater than 0.05 set as the level of significance, it, therefore, implies that the null hypothesis was not rejected.

4.2. Research question/hypothesis two

Table 3. ANOVA of the mean responses of administrative officers on the detective control measures adopted for effective information management

S/ no	The detective control measures		Nos of S = 45, T = 96, O = 139. Total Respondents = 280						
		$\bar{x}_S$	$\bar{x}_T$	$x_{\bar{O}}$	Rmk	Df	F-ratio	P-value	Rmk
1	Spot undesirable activities on the institutions' digital assets.	1.14	1.29	1.39	MA	319	1.32	0.47	NS
2	Use security alerts to assist in detecting malicious activities by unauthorized and unscrupulous persons on non-digital documents.	1.16	1.25	1.15	MA	319	1.19	0.39	NS
3	Install door alarms to detect unauthorized access to the confidential room where institutions' documents are housed.	1.14	1.17	1.15	MA	319	1.16	0.36	NS
4	Fix detective lights, and smoke and fire alarms around sensitive information zones.	1.27	1.16	1.36	MA	319	1.28	0.45	NS
5	Employ motion detectors and security guards around institutions' information centers.	1.35	1.30	1.41	MA	319	1.36	0.48	NS

6	Mount video surveillance around information centers and institutions' ICT facilities.	1.27	1.34	1.38	MA	319	1.35	0.48	NS
7	Enforce personnel vacations where necessary as a measure to detect fraudulent acts.	1.33	1.27	1.27	MA	319	1.28	0.45	NS
8	Use Intrusion Detection Systems to detect and report unauthorized access to institutions' digital assets.	1.20	1.25	1.27	MA	319	1.26	0.44	NS
9	Use Logs to authenticate users' access to institutions' digital documents and online environments.	1.29	1.36	1.25	MA	319	1.66	0.46	NS
10	Use Audit Trails to trace the detailed transactions relating to any item in an accounting record.	1.35	1.52	1.38	MA	319	1.42	0.49	NS
11	Use an access log and alert system to quickly detect fraud and notify management of any attempts by employees or unauthorized users to access institutions' information.	1.33	1.14	1.30	MA	319	1.25	0.43	NS
12	Use the reconciliations detective approach to compare different sets of information to identify if there is any variation from the original document.	1.39	1.18	1.27	MA	319	1.26	0.44	NS
13	Use management reviews to spot frauds and errors.	1.18	1.14	1.38	MA	319	1.26	0.44	NS
14	Use audits and financial reviews to spot unauthorized activities, mismanagement, or misappropriation of institutions' financial assets.	1.12	1.12	1.30	MA	319	1.74	0.41	NS
15	Use budgetary reviews and analysis to spot frauds.	1.14	1.20	1.23	MA	319	1.21	0.41	NS
16	Set up policies that support pre-approval of actions or transactions before processing such that any deviation from the standard can serve as a detective measure to spot fraud.	1.14	1.27	1.31	MA	319	1.27	0.44	NS
17	Use document control numbers to ensure that all transactions are recorded and accounted for.	1.04	1.12	1.42	MA	319	1.26	0.44	NS
18	Use computer passwords and access controls to avert unauthorized access to electronic or digital information.	1.08	1.15	1.20	MA	319	1.81	0.37	NS
19	Install intrusion detection systems around the information management department or unit.	1.35	1.32	1.31	MA	319	1.32	0.47	NS
20	Use intrusion detection systems software to monitor computer systems against malicious attacks, policy violations, and other prohibited intrusion or usage.	1.47	1.27	1.39	MA	319	1.36	0.48	NS
21	Use a firewall to filter connections against threats.	1.27	1.23	1.21	HA	319	2.34	0.42	NS
	Grand mean	1.24	1.24	1.30	MA	319	1.37	0.44	NS

The result in [Table 3] showed mean ratings ranging from 1.16 – 2.34 for all the items with a grand mean of 1.37 indicating that respondents moderately adopt the detective control measures except for item 21 which is highly adopted. The corresponding standard deviation to each of the items ranged from 0.36 – 0.49 with an overall of 0.44, signifying that the

opinions of the respondents were very close to one another on the level administrative officers adopt the detective control measures

Furthermore, [Table 3] showed the ANOVA result of the hypothesis of no significant difference among the mean responses of Strategic, Tactical, and Operational Administrative Officers on detective control measures adopted by them for effective information management in COEs in South-South Nigeria. The result revealed the p-value of all the items together with the overall p-value ranging from 0.37 – 0.49. Since the results of all the 21 items and the p-values are each greater than 0.05, it implies that the hypothesis (Ho2) is not significant. The hypothesis (Ho2) was therefore not rejected.

Based on the data analyzed, the study found that:

1. The administrative officers in colleges of education in South-South Nigeria highly adopted the procedural preventive control measures for effective information management of their institutions.
2. The administrative office in colleges of education in South-South Nigeria moderately adopted the identified detective control measures for effective information management.
3. Most of the information and communication control measures identified in this study were moderately adopted by the administrative officers of the colleges of education in South-South Nigeria.
4. The tested hypotheses showed that there was no significant difference among the mean responses of the Strategic, Tactical, and Operational Administrative Officers of the Colleges of Education in South-South Nigeria on the level at which they adopt the procedural preventive and detective control measures for effective information management of their institutions.

5. Discussion of findings

The discussion of the findings was done according to the specific control measures studied and the hypotheses tested.

5.1. Procedural preventive control measures for effective information management

The findings of this study on the procedural preventive control measures for effective information management were highly adopted. Among the procedural preventive control measures identified include: Put policies that support securing information assets such as hardware, software, and digital and non-digital resources of the institutions; Putting guiding rules that support restricting unauthorized access to ICT equipment, inventories, and other information assets; Mount strong physical securities in all aspect of the information system; Put surveillance and restricting access to confidential places where confidential documents are housed; Assign information officers on a routine basis to check through information assets and compared them the value shown on control records, and Use segregation of staff duties as a preventive control measure to protect institutional assets and resources among others.

The findings of this study are congruent with Dogan, [41] who noted that information management security is not merely an issue of technological advancements, hardware, and software, but includes understanding and managing staff and users who are covered by an institution's information both digital and non-digital. Again, the findings of this student are in agreement with Mendez [42] who maintained that procedural preventive control measures are

deliberately designed by organizations to deter errors, and irregularities and prevent fraudulent activities of malicious intruders. Similarly, the findings of the study on the usage of procedural preventive control measures as a tool for preserving institutional information assets for the achievement of organizational goals are in line with Mendez [42] and Abanyam, Ibelegbu, and Garba [43] who postulated that most institutions employ procedural preventive control measures as proactive controls that supports in ensuring that institutional goal and objectives are achieved. The findings of the study were also in line with the work of Janssen and Janssen [44] who found that procedural preventives control measures are fundamental framework control activities set forth by administrative staff to guide employees as they carry out their daily tasks. Mathews [38], Separation of Duties is the concept that states that in an organizational setup, the performance of a task requires that more than one person should be involved to complete the task. Also, the findings of the study supported the use of separation of duties to limit the amount of power and influence held by a staff identified by Coleman, [45]. In addition, the findings of the study strengthened the findings of Mathews [38] who further established that the performance of a task requires authorization from at least 2 staff to maintain integrity and security.

5.2. Detective control measures for effective information management

The findings of the study on detective control measures revealed that the administrative office in COEs in South-South do not highly but moderately adopt the identified detective control measures. By inference, the study established that the level at which the administrative officers adopted the identified detective control measures was not high enough to achieve effectiveness. Some of the detective control measures identified include: Spot undesirable activities on the institutions' digital assets; Use security alerts to assist in detecting malicious activities by unauthorized and unscrupulous persons on non-digital documents; Install door alarms to detect unauthorized access to a confidential room where institutions' documents are housed; Fix detective lights, smoke and fire alarms around sensitive information zones; Employ motion detectors and security guards around institutions' information centers; Mount video surveillance around information centers and institutions' ICT facilities; Enforce personnel vacations where necessary as a measure to detect fraudulent acts and Use Intrusion Detection Systems to detect and report unauthorized access to institutions' digital assets.

The findings of this study strengthened the findings of the University of California [35] which states that detective control measures provide evidence that a particular loss had occurred in an institutional information asset. Similarly, the findings are also in tune with Thomas et al. [36] who found in their study that detective control measures are designed to spot malicious and undesirable activities of hackers so that prompt actions can be taken before more serious harm is suffered. Again, the findings of this study were congruent with Thomas et al. [37] who found in their empirical study that though detective controls do not prevent intruders' attempts on institutional information if the control systems are effectively working, they help for easy detection of the ill attack, source and time of the attack occur. The findings of the study supported Thomas et al. [36] who also found in their study that some of the detective control measures institutions can adopt for effective detection of fraud and attacks on their information systems include: the use of Intrusion Detection Systems IDS for digital documents. Furthermore, the finding of this study agreed with Mathew [38] who postulated that institutions that have online platforms and portals can use Logs and Audit

Trails to detect when unauthorized users are attempting to hack into an information platform or site.

The findings of the study added value to the authenticity of the findings of Mathew [38] which identified that the following measures can be used as detective control for non-digital information: use of an alarm, fixing detective lights, application of motion detectors, putting security guards on duty at strategic positions where information assets are, use of video surveillance, and enforcing personnel vacations to checkmate errors and frauds.

Though this study has established that adoption of the procedural preventive and detective control measures are the keys to the survival of many institutions, there are some limitations to this study. First, the researcher used administrative officers in colleges of education in South-South Nigeria only. This has limited the generalization of the findings of the study to other administrative officers in tertiary institutions and organizations outside.

Secondly, the study was conducted in South-South Nigeria. This has limited the generalization of the findings of the study to other tertiary institutions in other geographical zones of the country and the world at large. Hence, it is suggested that a similar study should be conducted in other geographical zones of the country to determine if there will be any significant difference in the findings when compared with the findings of this study even using a different design to the one used for the study.

6. Conclusion

This study investigated the control measures adopted by administrative officers for effective information management in COEs in South-South Nigeria. Based on the findings of the study, it is inferred that the level of adoption of the identified information control measures by the administrative officers of the COEs in South-South Nigeria is not high. This could be among the reasons why the information in the colleges is highly vulnerable to several online threats and malicious attacks. It is established in this study that effective information management through procedural preventive, and detective control measures is the key to the survival of the institutions from unscrupulous hackers. Diligent application of the identified control measures will also help the administrative officers to check-mate against internal errors, frauds, and abuse of information by staff and students. Above all the statutes, integrity, and standard of the institutions will improve if the information control measures are effectively implemented. It is, therefore, imperative for the stakeholders of COEs in Nigeria to take seriously issues of adaptation of control measures for effective information management in the institutions.

7. Recommendations

Based on the findings of this study, the following recommendations were made:

1. Administrators and management of COEs in Nigeria should enact effective policies and laws that support the adaptation of procedural preventive control measures in their institutions.
2. The management of COEs should provide 21st-century ICT equipment that has updated applications that guarantee detective control measures.
3. Since security is the responsibility of everyone, the Director of Academic Planning should organize training in form of conferences, seminars, symposiums, and

workshops for academic and teaching staff as well as students on the general information control measures.

4. This study should be replicated in other zones of the country, parastatals, government ministries, and related areas using other control measures such as monitoring, recovery, and logical controls to reduce administrative damages.
5. There is a need for an in-depth study to be conducted on exploring the operational barriers that impede tertiary institutions from implementing information security controls.

Acknowledgment

The researchers did not receive any grant or support from any funding agency. However, the authors appreciate our respondents and the university authorities for giving us enabling platforms to successfully carry out this research work.

References

[1] National Commission for Colleges of Education, "Nigeria certificate in education minimum standards for general education courses, TETF project 2012," Department of Academic Programmes, Garki, Abuja, **(2019)**

[2] [E. E. Agomuo, "Modern office technology: Issues, procedures, and practice," Debees Printing Services, Nsukka: pp.67-98, **(2014)**

[3] E. C. Osuala and A. U. Okeke, "Administrative office management," Cheston Agency Ltd., Enugu, pp.56-79, **(2006)**

[4] B. Ezeali and U. Ewulonu, "Office management and organizations (Theories and Applications)," Chambers Books Limited at Chambers Press Limited. Onitsha, pp. 54-66, (**2011)**

[5] M. Johnson, "What are business operations?" https://resources.work.com, (2009), https://resources.work.com/administrative-officer-job-description.

[6] F. E. Abanyam and E. T. Guma, "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, vol.1, no.1, pp.42-54, **(2021)**

[7] H. W. J. Meyer, "Information use in rural development," The New Review of Information Behavior Research, vol.4, pp.109-126, **(2003)**

[8] J. P. Jumper, "Levels of air force leadership," https://www.doctrine.af.mil**, (2005),** https://www.doctrine.af.mil/Portals/61/documents/Volume_2/V2-D10-Levels-Leadership.pdf.

[9] R. Martin, "The three levels of leadership," https://exploitingchange.com, (2011), https://exploitingchange.com/2011/02/28/the-three-levels-of-leadership/, Applications, Onitsha: Chambers Books Limited at Chambers Press Limited. 978-63519-1-7

[10] K. Mikoluk, "Planning in management: strategic, tactical, and operational plans," https://blog.udemy.com, **(2013)**, https://blog.udemy.com/planning-in-management/

[11] The state of Vermont, "Monitoring, assessment and planning," https://dec.vermont.gov, (2015), https://dec.vermont.gov/watershed/map

[12] T. Lucey, "Management information systems," Seng Lee Press, Singapore, **(2005)**

[13] J. Q. McCrindell, "Framework for financial management and control," Journal of Finance Management Institute, vol.16, no.2, pp.11-39, **(2015)**

[14] State of New York Comptroller, "Standards for internal control in New York State government," **(2007)**, https://osc.state.ny.us/agencies/ ictf/docs/intcontrol_stds.pdf.

[15] J. A. Mattie, P. F. Hanley, and D. L. Cassidy, "Internal controls: The key to accountability," www.ucop.edu, (2005), www.ucop.edu/riskmgt/ erm/documents/ pwc_int_ctrls.pdf.

[16] R. Gauthier, "Major event legislation: Lessons from London and looking forward," The International Sports Journal, vol.14, no.1-2, pp.58-71, **(2014)**

[17] The Institute of Internal Auditors, "Practice guide: Auditing the control environment," https://na.theiia.org, (2008), https://na.theiia.org/standards-guidance/ recommended-guidance/practice-guides/Pages/Auditing-the-Control-Environment-Practice-Guide.aspx.

[18] M. Fabunmi, "Perspective in educational planning," Odun Printers and Pack, Ibadan, **(2006)**

[19] A. Neelameghan, "Information systems for national development - The social relevance of information systems," International Forum on Information and Documentation, vol.5, no.4, pp.3-8, **(2008)**

[20] B. Mellon, "US research universities increasingly targeted by cyber-attacks," http://www.upi.com, (2013), http://www.upi.com/Top_News/US/2013/07/17/US-research-universities-increasingly-targeted-bycyberattacks/26641374065244/

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

[22] Africa Cyber Security. "African universities battle hacking, cybercrimes," https://punchng.com, (2016), https://punchng.com/african-universities-battle-hacking-cyber-crimes/

[23] G. Rogers and T. Ashford, "Mitigating higher-end cyber-attacks," ASCUE Proceedings, vol.5, no.2, pp.234-241, **(2015)**

[24] S. Chand, "Decisions making: Strategic, tactical and operational decisions and business management," http://www.yourarticlelibrary.com, (2019), http://www.yourarticlelibrary.com/informationtechnology/decisions-making-strategic-tactical-and-operational-decisions-business-management/10271

[25] A. Bytheway, "Investing in Information: The information management body of knowledge," Springer, Geneva, **(2015)**

[26] Techopedia, "Information management (IM)," https://www.techopedia.com, (2019), https://www.techopedia.com/definition/20012/information-management-im

[27] F. E. Abanyam, "Self-employment skills possessed by business education students of colleges of education for sustainable development in Cross River State," M. Ed thesis, Department of Business Education, University of Nigeria Nsukka, Nigeria, **(2014)**

[28] T. Oyedepo, and N. Okorie, "Public relations and internet usage: A strategic approach to promoting corporate image and identity," International Journal for Social Sciences and Humanities," vol.4, no.1, pp.64-73, **(2011)**

[29] O. Tunji and O. Nelson, "The effect of e-portal system on the corporate image of universities," i-manager's Journal of Educational Technology, vol.7, no.4, pp.345-349, **(2011)**

[30] C. Bradford, "Examples of IT detective controls," https://yourbusiness.azcentral.com, (2019), https://yourbusiness.azcentral.com/examples-detective-controls-10984.html.

[31] National Vulnerability Database, "Security and privacy controls for federal information systems and organizations," https://nvd.nist.gov, (2019), https://nvd.nist.gov/800-53/Rev4/control/SI-4

[32] State of New York Comptroller, "Standards for internal control in New York State government," https://osc.state.ny.us, (2007), https://osc.state.ny.us/agencies/ ictf/docs/intcontrol_stds.pdf.

[33] G. Misra, "Office operations: Meaning, importance, and classification," http://www.yourarticlelibrary.com, (2019), http://www.yourarticlelibrary.com/office-management/office-operations-meaning-importance-and-classification/74657.

[34] R. Acharya, V. Vityanathan and R. Pether, "Wireless LAN security – Challenges and solutions", International Journal of Computer and Electrical Engineering, vol.1, no.3. **(2009)**

[35] The University of California, "Understanding internal controls," (2017), http://www.universityofcaliforna.com

[36] A. I. Thomas, T. Cavanaugh A. Lydia, T. Williams, and A. Taylor, "Internal controls compliance office of business affairs," https://www.pvamu.edu, (2008), https://www.pvamu.edu/universitycompliance/wp-content/uploads/sites/87/PVAMU-Internal-Control-Training.pdf.

[37] C. Thomas, V. Sharma, and N. Balakrishnan, "Usefulness of DARPA data set for intrusion detection systems evaluation," Proc. of the SPIE, Defense and Security Symposium, Mar. **2008**

[38] J. Mathews, "Job description of an administrative operations manager," https://classroom.synonym.com, (2019), https://classroom.synonym.com/job-description-administrative-operations-manager-8397498.html

[39] F. E. Abanyam and V. A. Abanyam, "Green marketing in South-South Nigeria consumer sustainability: The distribution and physical practice on polythene manufacturing companies," Journal of Contemporary Issues and Thought, vol.1, no.1, pp.126-140, **(2021)**

[40] S. Cooper, "Best intrusion detection systems (10+ IDS Tools," https://www.comparitech.com, (2019), https://www.comparitech.com/net-admin/network-intrusion-detection-tools/

[41] S. Dogan, "Perceptions of teachers about the use of educational technologies in the process of instruction," Odgojne znanosti, vol.12, no.2, pp.134-146, **(2010)**

[42] R. Mendez, "General control vs. application control. Prezi," https://prezi.com, (2015), https://prezi.com/iacknmfi6oxg/general-control-vs-application-control/

[43] F. E. Abanyam, A. N. Ibelegbu, and H. J. Garba, "Green marketing: The entrepreneur and compliance marketing approaches for predicting sustainable industries in South-South Nigeria," Vocational and Technical Education Journal, vol.4, no.2, pp.265-277, **(2020)**

[44] D. Janssen and C. Janssen, "Electronic data interchange," https://www.techopedia.com, (2019), https://www.techopedia.com/definition/1496/electronic-data-interchange-edi

[45] K. Coleman, "The key to data security: Separation of duties. Computer world," https://www.computerworld.com, (2008), https://www.computerworld.com/article/2532680/the-key-to-data-security--separation-of-duties.html.

[46] G. Rogers and T. Ashford, 'Mitigating higher ed cyber-attacks," ASCUE Proceedings, vol.5, no2, pp.234-241, **(2015)**