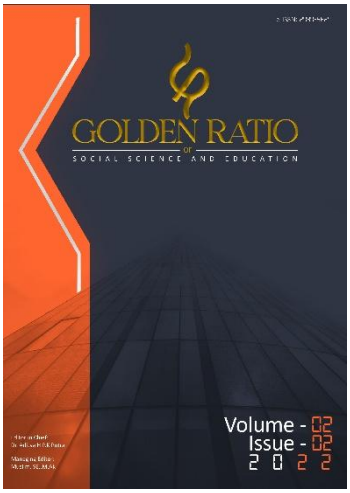
https://doi.org/10.52970/grsse.v2i2.183

Website: https://goldenratio.id/index.php/grsse/index

OPEN ACCESS

ISSN [Online] 27975827



Received: May 02, 2022
Revised: May 14, 2022
Accepted: November 30, 2022

*Corresponding author: Friday Ekahe Abanyam, Department of Business Education, Faculty of Education, Ambross Alli University, Ekpoma, Edo State, Nigeria.

E-mail: fabanyam@aauekpoma.edu.ng

SOCIAL SCIENCE AND EDUCATION | RESEARCH ARTICLE

Information and Security Control Mechanisms Embraced for Effective Information Management in Colleges of Education in Nigeria

Augustine Naboth-Odums[1], Friday Ekahe Abanyam[2*], Abdulrahman Abdulkadir[3], Victor Attah Abanyam[4]

[1] School of Business Education, Federal College of Education (Technical) Omoku, River State, Nigeria. Email:naboth-odumsaustin@gmail.com
[2] Department of Business Education, Faculty of Education, Ambross Alli University, Ekpoma, Edo State, Nigeria. Email: fabanyam@aauekpoma.edu.ng
[3] School of Business Education, Federal College of Education (Technical) Gombe, Gombe State, Nigeria. Email:balaab@fcegombe.edu.ng
[4]Department of Vocational Education, Faculty of Education, University of Calabar, Calabar, Cross River State, Nigeria. Email: vabanyam@gmail.com

Abstract: The study determined the Information, communication and logical environment security control mechanisms embraced by administrative officers for effective information management in Colleges of Education (CCOEs) in South-South Nigeria. The study embraced descriptive survey research design. The population was 1580 Administrative Officers.. 320 respondents using a proportional sampling technique was used to determine the number of administrative officers for each of the COEs 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 administrative officers moderately embraced the identified logical, information and communication control mechanisms 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 embraced the Information, communication and logical environmental security control mechanisms for effective information management of their institutions. it was recommended among others, that the management of COEs in Nigeria should enact and implement effective policies and laws that support the adoption of information control mechanisms.

Keywords: Communication, Logical Environment Security, Control Mechanisms, Information Management, Education.

1. INTRODUCTION

Colleges of Education (COEs) are among the tertiary institutions in Nigeria that were established by 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, junior secondary school levels and/or proceed to university education. COEs programmes are run for a period of three years including four months Student Industrial Work Experience Scheme and six months teaching practice (National Commission for Colleges of Education, 2019). The author posited that NCE programme was introduced to prepare individuals to become leaders and practitioners in education and in related human service fields by expanding and deepening understanding of education as a fundamental human right. In order 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.

https://doi.org/10.52970/grsse.v2i2.183
Website: https://goldenratio.id/index.php/grsse/index
ISSN [Online] 27975827

Administrative offices serve as support units to all other departments in COEs in Nigeria. The administrative office, according to Agomuo (2014), is a place where clerical functions necessary for information handling is carried out. Similarly, Osuala and Okeke (2006) 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. In order 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 (Ibelegbu & Abanyam, 2022). 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, information on security and human resource matters.

Administrative office operations are concerned with the coordination of finance, and operational performance of routine office tasks (Johnson, 2009). This involves handling of information appropriately on daily basis. According to Abanyam and Guma (2021), 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 of 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 with regard to fiscal and other matters. According to Meyer (2003), administrative officers are the greatest resource of COEs 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 COEs must be beneficial from the way administrative officers manage information. In `management, there are three major classifications of managerial levels, namely: strategic, tactical and operational levels (Mikoluk, 2013; Martin, 2011; Jumper, 2005). This classification is based on functions and responsibilities of the administrative officers.

The levels of management are traditionally represented as strategic, tactical and operational (Osuala, & Okeke, 2006). The authors added that the strategic mangers 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 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 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, cost, 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 are able to 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 State of Vermont (2015), 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 make informed decisions, determine their risks, and communicate policies and other important information to those who require it. State of Vermont (2015) 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 effective of information systems in COEs with the sole aim of achieving the institutions' set goals. Effective information

https://doi.org/10.52970/grsse.v2i2.183
Website: https://goldenratio.id/index.php/grsse/index ISSN [Online] 27975827

management involves the application of administrative control mechanisms to ensure that information is properly processed, secured and delivered as at when due.

Administrative control is a critical function of management. It comprises policies, plans, procedures and practices used to manage the organization and meet the organizations goals and objectives (Lucey, 2005). They serve as means of managing the risks associated with programmes and operations. According to Lucey, 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 organization. In this study, administrative control is the process of ensuring that actual activities of the COEs in relation to 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.

There are several administrative controls that can be embraced 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 mechanisms (McCrindell, 2015; State of New York Comptroller, 2007); logical security and environmental control (Mattie, Hanley & Cassidy, 2005); storage, information communication, environment (physical), and monitoring controls (Gauthier, 2014; The Institute of Internal Auditors, 2008); and recovery control mechanisms (Neelameghan, 2008; Fabunmi, 2006). In this study however, logical security and information communication and information communication controls shall be of interest to the researchers.

2. LITERATURE REVIEW

2.1. Information and Communication Control Mechanisms

Most of the COEs in Nigeria use a variety of information and communication systems in their daily operations and activities. Some of the ICT systems used in institutions include: mainframe computers, laptops, minicomputers, personal computers, single-user workstations, telephone systems, video conference systems, local area networks and wide area networks, among others. The need for designing information communication control over these systems depends on the extent to which the information is critical and confidential. It also depends on the complexity of the network and applications that the institution is using on the systems. According to University of California (2017), there are basically two broad categories of controls that can be set for information systems. They include: general control and application control. In the opinion of Kenneth, Laudon, and Laudon (2014), general control concerns the whole information systems and all the applications/software that reside on the information systems. This type of control includes: Data & program security, access security, physical security; data center operations, application software development and program change controls as well as disaster recovery.

General controls involve all practices designed to sustain the integrity and availability of information systems, networks, information processing functions, and associated software systems (Mendez, 2015; Kenneth et al., 2014). It is concerned with institutions' application processing that ensures and guarantees complete and accurate information processing. The major intent of this system is to ensure that information is processed, and processing diagnostics, frauds, and errors are observed and resolved. On the other hand, application control is a system that focuses on computer software, its protection and security. Applications or software refers to the computer system programs and processes that help one carry out activities on computer systems. It supports activities such as financial transactions, online payments, accounting, forecasting and monitoring of personal or institutional budgets (Mendez, 2015). Furthermore, information officers can also use electronic data interchange, voice response, and expert systems to secure their online transactions and communications. In recent years, institutions have their online portals through which different kinds of financial transactions hold. Students generate school fees, hostel fees and other bursary fee invoices and pay online; institution with other institutions enter business relationship, units, centers,

https://doi.org/10.52970/grsse.v2i2.183
Website: https://goldenratio.id/index.php/grsse/index ISSN [Online] 27975827

department, schools interact using online portals and platforms. All these forms of transaction are supported by Electronic Data Interchange (Janssen & Janssen, 2019).

Electronic Data Interchange (EDI) is the transfer of information or data from a source computer system to another (receiver) through a standardized message formatting without human intervention (Rouse, 2014). Rouse argued that since institutions engage in series of online activities and transactions, it is very important their information officers must ensure that the transaction systems or applications have sufficient application controls such as input controls, processing controls, and output controls. Input controls, according to Janssen and Janssen (2019), helps information officers ensure that there are complete and accurate entries of authorized transactions by authorized users only. It also helps to identify suspended, rejected, and duplicate items; and to resubmit rejected and suspended items electronically. Again, processing controls helps in ensuring that there is a complete and accurate processing of authorized transactions. Some of the examples of processing control systems include: posting checks, control files, run-to-run control totals, end-of-file procedures, concurrency controls, and audit trails (Janssen & Janssen, 2019). Finally, output controls help to ensure that total and accurate audit trail of the outcomes of processing control is reported to appropriate persons for review. In addition to general control, application control, and EDI, institutions should employ other security tools to secure end-user access to their vital platforms in digital environment. One of such tool is encryption keys.

Cryptography is very important in both digital and non-digital worlds. In non-digital world (i.e. physical world with no computers, email, no iPads, and no electronic devices) there are range of security mechanisms that can be used to guide and preserve institution's data and information. In non-digital world are often presented in spoken form and written form, thus, this information is represented physically in terms of objects. Security for such information is secrecy restriction of who can access them. Martin (2011) noted that spoken words can be protected by communicating parties whispering to each other. Information in form of spoken words during a meeting can as well be kept secret by shutting the doors such that only those present and are inside the room can hear the conversation, while people outside the room cannot. This implies that physical presence can often be used to guide secrecy. However, information that is written down can be guided using range of techniques. Among the technics include: put letters in envelopes and inserting a seal on the envelope. Martin (2011) argued that the actual seal on the envelope is basically a property which allows an information officer to detect if someone has opened the document or changed the contents. The author also added that written information can be secured by keeping them in a filing cabinet and using a lock to secure them in the cabinet.

Cryptography is a tool kit of tools of mechanisms that provide different types of security in the digital world. In digital world, one most obvious property that an institution must consider while making attempt to secure its digital information is secrecy. Information secrecy demands that only designated recipients can learn the contents of information. This involves confidentiality of information i.e. making sure information is restricted only to intended participants or users. To achieve effective cryptographic security and confidentiality of institutions' documents, encryption is used. Encryption is required in modern day information security to avert heavy loss, attack and fraud.

Confidentiality of digital information can be achieved using the following cryptographic tools: block cyphers, string cyphers, public key encryption. Another tool required to secure digital world is data integrity. Data integrity is an assurance that data has not been altered or changed either accidentally or deliberately before someone actually reads it or relies on it. Cryptographic tools for providing data integrity vary in the strength of integrity that they provide. Data integrity tools include: hash functions, message authentication codes, and digital signatures (Martin, 2011). According to the author, a hash function is a tool that detects accidental changes to data. Stronger data integrity demands for a stronger property than data integrity and the tool for securing such data is origin authentication (message authentication). The origin authentication not only ensures that data has not been changed, but actually provides some kind of assurance as to who sent the data. This is sometimes referred to as message authentication. This is an effective tool that provides information officers with the ability to check that the data has not been changed and also gives some insurance as to where changes came from in situation where such has occurred.

https://doi.org/10.52970/grsse.v2i2.183
Website: https://goldenratio.id/index.php/grsse/index
ISSN [Online] 27975827

2.2. Logical Environment Security Control Mechanisms

Logical environment security controls refer to technical controls. Northcutt noted that logical security controls involve the use of software and data to monitor and control access to information and computing systems (Techopedia, 2019). Still in National Vulnerability Database (2019), there are technical and administrative mechanisms to avoid counteract or minimize loss of information due to the workers' vulnerability. For instance, passwords, network and host-based firewalls, network intrusion detection systems, access control lists, and data encryption are logical security controls mechanisms to safe guard information (Abanyam, Ibelegbu, & Garba, 2020; Misra, 2019). François (2016) pointed out that specific control activities include frequent changes of dial-up numbers; use of dial-back access; restrictions on users to allow access only to system functions that they need; software and hardware "firewalls" to restrict access to assets, computers, and networks by external persons; and frequent changes of passwords and deactivation of former employees' passwords. Controls mechanisms are required for interfaces to verify inputs and outputs; such as edit checks. General and application control over information systems are interrelated, and are required to ensure complete and accurate information processing.

The control environment is the control consciousness of an organization; it is the atmosphere in which people conduct their activities and carry out their control responsibilities. According to University of California (2017), an effective control environment is an environment where competent staff understands their responsibilities, the limits to their authority, and are knowledgeable, mindful, and committed to doing what is right and doing it the right way and at the right time. The author added that in control environment, workers are committed to following an organization's policies and procedures and its ethical and behavioral standards. The control environment encompasses technical competence and ethical commitment; it is an intangible factor that is essential to effective internal control. It is the responsibility of institutions' governing board and management to enhance an institutions' control environment by establishing and effectively communicating written policies and procedures, a code of ethics, and standards of conduct for staff to align. Moreover, a governing board and management of an institution enhance the control environment when they behave in an ethical manner i.e. by creating a positive leadership stand and ensure that the standard, they set is followed by all the staff. It is the role of the management to create a control environment that fosters: the high levels of institutional integrity, personal and professional standards (Abanyam et. al., 2020).

According to the Institute of Internal Auditors (2008), control environment comprises a collection of an entity's organizational structure, policies, processes, and standards that are used to maintain control across the entire institution. The author further pointed out that it is the sole responsibility of the board of directors and executive management of an institution to set the culture and attitude about the importance of maintaining controls and also to set the expectations of standards of conduct within the institution. this standard is often regarded as "the tone at the top." There are five major principles regarding to a control environment. They are: i) establishing a commitment to Integrity and Ethical Values for the institution, ii) maintaining an independence of the board of directors from management and their oversight of the institutions' internal control, iii) establishing organizational structure, authority, reporting lines, and responsibilities to pursue the institutions' core objectives, iv) establishing a commitment to attract, develop, and maintain competent staff, and v) maintaining serious accountability for the execution of internal control responsibilities (Acharya, Vityanathan, & Pether, 2009).

The control environment mechanisms set the tone of an organization, influencing the control consciousness of its people. The control environment is influenced by institutional philosophy, operating style, integrity, ethical values, and commitment to competence. Control environment factors include the integrity, ethical values, and competence of the staff; management philosophy and operating style; and the way management assigns authority, organizes and develop its people (National Vulnerability Database (2019). If the control environment is positive, the overall system of information management will be more effective.

The demand for effective information security measure is an urgent need in tertiary institutions in Nigeria especially and the world at large. This is because there are several cases of attacks

https://doi.org/10.52970/grsse.v2i2.183
Website: https://goldenratio.id/index.php/grsse/index ISSN [Online] 27975827

occurring on daily basis on institutional information systems (Abanyamm & Abanyam, 2021). 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 Ewepu (2016), as of 2016, Nigeria is ranked 16th highest country in cyber-attacks vulnerabilities in Africa.

Several tertiary institutions have suffered cyberattack in African including Nigeria. According to a report by Africa Cyber Security (2016), 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 (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 control mechanisms, failure to patch and secure institutional information systems. Based on this background, the questions of what entails information and communication as well as logical environment security control mechanisms embraced by administrative officers for effective information management would be provided in this study. We therefore developed the following null hypotheses to guide the study:

H1: There is no significant difference in the mean responses of strategic, tactical, and operational administrative officers on the information and communication control mechanisms embraced for effective information management.
H2: There is no significant difference in the mean responses of strategic, tactical, and operational administrative officers on the logical environment security control mechanisms embraced for effective information management.

3. Research Method and Materials

This study embraced 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 [6]. This design is therefore considered suitable for this study because it makes use of questionnaire to collect data from the respondents on logical, information and communication control mechanisms embraced 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 main stay 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 in relation to 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, 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 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 good position to respond to questions about the administrative information on control mechanisms embraced 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 [38] was used to determine the sample size of the respondents from the COEs being studied. After determining the sample size,

https://doi.org/10.52970/grsse.v2i2.183
Website: https://goldenratio.id/index.php/grsse/index
ISSN [Online] 27975827

proportionate sampling technique was used to determine the number of the strategic, tactical and operational administrative officers for each of the COEs studied.

The instrument used for data collection was structured questionnaire titled "Information management Control Mechanisms Questionnaire (IMCMQ)" developed by the researcher. The questionnaire sought information on the logical, information and communication control mechanisms embraced by administrative officers for effective information management in COEs with 18 and 22 items respectively and was structured on a 4-point scale with response options of very highly embraced (VHE), highly embraced (HE), moderately embraced (ME), and lowly embraced (LE) 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 COEs 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 0.93 for information and communication, and 0.96 for logical environment security control mechanisms with an overall coefficient of 0.93.

The researcher with the help of eleven (11) research assistants, one for each of the 11 Federal and State COEs in South – South administered the questionnaire to the respondents. The researchers found it challenging to obtained responses from some of the strategic administrative officers who out 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. Where the participants were willing to be involved in the study, some of them complained of the 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 actually 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 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 Embraced (VHE)	4	3.0 – 4.0
2	Highly Embraced (HE)	3	2.0 – 2.9
3	Moderately Embraced (ME)	2	1.0 – 1.9
4	Lowly Embraced (LE)	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 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. RESULTS AND DISCUSSION

4.1. Research Question/Hypothesis One

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.

https://doi.org/10.52970/grsse.v2i2.183

Website: https://goldenratio.id/index.php/grsse/index

ISSN [Online] 27975827

Table 2. ANOVA of the mean responses of administrative officers on the information and communication control mechanisms

S/N	The information and communication control mechanisms	Nos of S = 45, T = 96, O = 139. Total Respondents = 280							
		x_S	x_T	x_O	Remarks	Df	F-ratio	P-value	Rmk
1	Carry out file backups at regular intervals to protect digital documents.	1.39	1.33	1.14	ME	319	1.81	0.44	NS
2	Use disaster planning to ensure successful recovery and continuity of information system networks and information processing in the event of any disaster.	1.29	1.31	1.24	ME	319	1.27	0.44	NS
3	Use application controls like input controls, validation, error notification, to detect, prevent, and correct errors and irregularities in transactions flow in institutions' information systems.	1.35	1.33	1.28	ME	319	1.31	0.46	NS
4	Use processing and output controls mechanisms to ensure that all online transactions and programs are fully secured.	1.22	1.14	1.32	ME	319	1.24	0.43	NS
5	Print confidential documents and sensitive documents like certificates, letterhead papers on special papers with unique signs, logo or marks.	1.18	1.24	1.41	ME	319	1.52	0.37	NS
6	Protect sensitive documents like certificates, letterhead papers by covering them with water marks with holograms.	1.27	1.21	1.14	ME	319	1.79	0.39	NS
7	Use block cyphers, string cyphers, public key encryption to secure digital world.	1.37	1.25	1.23	ME	319	1.26	0.44	NS
8	Use string cyphers to secure digital world and to maintain data integrity.	1.61	1.16	1.17	ME	319	1.23	0.42	NS
9	Use string cyphers to secure institutions' digital documents.	1.47	1.18	1.24	ME	319	1.25	0.43	NS
10	Use public key encryption to secure digital world and to restrict unauthorized access to institutional digital assets.	1.41	1.18	1.31	ME	319	1.28	0.45	NS
11	Set block cyphers to secure digital world of the institutions' information assets.	1.43	1.32	1.24	ME	319	1.29	0.46	NS
12	Use string cyphers encryption to protect digital data and cyber information of the institution.	1.39	1.24	1.27	ME	319	1.28	0.45	NS
13	Set public key encryption to lock out unauthorized access to institutional information database.	1.55	1.36	1.24	ME	319	1.33	0.47	NS
14	Use data integrity assurance to ensure that no alteration or accidental or deliberate change on data before someone actually reads it.	1.20	1.18	1.25	ME	319	1.22	0.41	NS
15	Use input controls like key	1.10	1.22	1.29	ME	319	1.23	0.42	NS

https://doi.org/10.52970/grsse.v2i2.183

Website: https://goldenratio.id/index.php/grsse/index

ISSN [Online] 27975827

S/N	The information and communication control mechanisms	Nos of S = 45, T = 96, O = 139. Total Respondents = 280							
		x_S	x_T	x_O	Remarks	Df	F-ratio	P-value	Rmk
	verification and key matching to ensure complete and accurate entries of authorized transactions by authorized users only in the instructions' digital environment.								
16	Use sequence check to verify ordered data	1.18	1.30	1.29	ME	319	1.27	0.44	NS
17	Use File and Data Transmission Controls to ensure that internal and external electronically transmitted files and transactions are received from an identified source and processed accurately and completely.	1.06	1.28	1.32	ME	319	1.26	0.45	NS
18	Use Master Files and Standing Data Controls to ensure the integrity and accuracy of master files and standing data.	1.12	1.24	1.40	ME	319	1.30	0.50	NS
	Grand mean	**1.27**	**1.24**	**1.31**	**ME**	**319**	**1.34**	**0.44**	**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, A= Embraced, MA = Moderately Embraced

The result in Table 2 showed the mean ratings ranging from 1.22 – 1.81 with a grand mean of 1.34 indicating that level at which the respondents (Strategic, Tactical and Operational Administrative Officers) embrace the information and communication control mechanisms was moderate. Similarly, the corresponding standard deviation to each of the items ranged from 0.37 – 0.50 with an overall of 0.44, signifying that the opinions of the respondents were very close to one another on the level at which they adopt the information and communication control mechanisms.

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 information and communication control mechanisms embraced by them for effective information management in COEs in South-South Nigeria. The result revealed a cluster F-value of 1.34 with a significant value (P-value) of 0.44 and the p-values for each of the items ranged from 0.37-0.47. Since the result of item 1 to 18 and all the p-values are each greater than 0.05 set as level of significance, the null hypothesis (Ho3) was not rejected.

4.2. Research Question/Hypothesis Two

Table 3. ANOVA of the mean responses of administrative officers on the logical environment security control mechanisms embraced for effective information management

S/no	The Logical environment security control mechanisms	Nos of S = 45, T = 96, O = 139. Total respondents = 280							
		x_S	x_T	x_O	Remarks	Df	F-ratio	P-value	Rmk
1	Demonstrate a commitment to integrity and ethical value by setting up standard of conducts.	1.14	1.30	1.29	ME	319	2.45	0.09	NS
2	Maintain the independence of the board of directors from management and their oversight of the entity's internal control	1.16	1.22	1.50	ME	319	17.77	0.00	S
3	Establish organizational structure, reporting lines, authority, and responsibilities to pursue	1.10	1.30	1.12	ME	319	8.58	0.00	S

https://doi.org/10.52970/grsse.v2i2.183

Website: https://goldenratio.id/index.php/grsse/index

ISSN [Online] 27975827

S/no	The Logical environment security control mechanisms	Nos of S = 45, T = 96, O = 139. Total respondents = 280							
		x_S	x_T	x_O	Remarks	Df	F-ratio	P-value	Rmk
	institution's objectives.								
4	Demonstrate a commitment to attract, develop, and maintain competent staff through constant trainings on information management.	1.26	1.15	1.17	ME	319	9.16	0.00	S
5	Maintain accountability standard for the execution of internal control responsibilities.	1.20	1.35	1.32	ME	319	1.75	0.18	NS
6	Specify appropriate objectives to support effective environmental control mechanisms.	1.41	1.36	1.29	ME	319	1.57	0.21	NS
7	Identify and analyze risks	1.51	1.34	1.25	ME	319	6.21	0.00	S
8	Evaluate fraud risks by checking the sources and causes of the risk as well as the weak points in the information systems.	1.02	1.26	1.29	ME	319	8.17	0.00	S
9	Identify and analyze changes that could significantly affect internal controls	1.24	1.33	1.35	ME	319	0.95	0.39	NS
10	Set up control activities that will help to mitigate risks.	1.14	1.26	1.38	ME	319	5.89	0.00	S
11	Develop technology controls to ensure that information systems are often checked against errors and malfunctioning.	1.37	1.39	1.43	ME	319	0.32	0.73	NS
12	Deploy control activities that are in line with policies and procedures of the institution.	1.35	1.43	1.34	ME	319	1.13	0.32	NS
13	Use relevant, quality information to support the internal control function.	1.37	1.35	1.18	ME	319	6.64	0.00	S
14	Communicate internal control information internally.	1.31	1.29	1.25	ME	319	0.45	0.64	NS
15	Communicate internal control information externally.	1.24	1.32	1.22	ME	319	1.73	0.18	NS
16	Perform ongoing or periodic evaluations of internal controls (or a combination of the two).	1.33	1.31	1.16	ME	319	5.38	0.01	S
17	Communicate internal control deficiencies.	1.35	1.32	1.17	ME	319	6.07	0.00	S
18	Communicate internal control strength to maintain.	1.39	1.40	1.25	ME	319	4.21	0.02	S
19	Use internal audit and/or compliance function to assessing and maintaining institution's control environment.	1.49	1.39	1.18	ME	319	12.16	0.00	S
20	Employ personnel with the experience and skill-sets specific to information management and security.	1.16	1.34	1.31	ME	319	2.70	0.07	NS
21	Engage external entities periodically to assess the environment to provide management with an accurate picture of the institution's control	1.24	1.43	1.27	ME	319	4.87	0.01	S

https://doi.org/10.52970/grsse.v2i2.183

Website: https://goldenratio.id/index.php/grsse/index

ISSN [Online] 27975827

S/no	The Logical environment security control mechanisms	Nos of S = 45, T = 96, O = 139. Total respondents = 280							
		x_S	x_T	x_O	Remarks	Df	F-ratio	P-value	Rmk
	environment.								
22	Use incentives to motivate staff so that they can render quality services and ensure environmental security of the institution's information resources.	1.26	1.33	1.27	ME	319	14.98	0.00	S
	Cluster mean	**1.28**	**1.33**	**1.27**	**ME**	**319**	**5.60**	**0.13**	**NS**

The result in Table 3 showed mean ratings of the items ranging from 1.24 – 1.88 with a grand mean of 1.52 indicating that the Administrative Officers moderately embraced the logical environmental security control mechanisms, except for the items 2 and 3. The items 2 and 3 with mean 2.35 and 2.18 respectively were highly embraced. On the other hand, 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 embraced the logical environmental security control mechanisms.

The result in Table 3 also showed the ANOVA result of the hypothesis of no significant difference among the mean responses of Strategic, Tactical and Operational Administrative Officers on logical environment security control mechanisms embraced by them for effective information management in COEs 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 2, 3, 4, 7, 8, 10, 13, 16, 17, 18, 19, 21 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 (Ho2) was not rejected. Based on the data analyzed, the study found that:

1. The administrative officers in COEs in South-South Nigeria moderately embraced the Information and Communication control mechanisms for effective information management of their institutions.
2. The administrative officers in COEs in South-South Nigeria moderately embraced the identified logical control mechanisms for effective information management.
3. The tested hypotheses showed that there was no significant difference among the mean responses of the Strategic, Tactical and Operational Administrative Officers of the COEs in South-South Nigeria on the level at which they adopt the Information and Communication and logical control mechanisms for effective information management of their institutions.

4.3. Discussion

The study found that most of the information and communication control mechanisms identified in this study were not highly embraced by the administrative officer of the COEs in South-South, Nigeria. Therefore, by inference, the study established that the level of the adoption of the information and communication control measure by the information officers were at the moderate level. Some of the Information and Communication control mechanisms identified include: carry out file backups at regular intervals to protect digital documents; use disaster planning to ensure successful recovery and continuity of information system networks and information processing in the event of any disaster; use processing and output controls mechanisms to ensure that all online transactions and programs are fully secured amongst others. These findings are congruent with Mendez (2015) and Kenneth et. al. (2014) who found that information and communication control mechanisms cover computer operations control, hardware controls, software controls, data security controls, systems implementation controls and process. This implies that administrative officers in educational institutions, including COE can use electronic data interchange, voice response, and expert systems to achieve and effective information management of their online transactions

https://doi.org/10.52970/grsse.v2i2.183
Website: https://goldenratio.id/index.php/grsse/index ISSN [Online] 27975827

Similarly, institutions can protect their private and very sensitive documents such as certificates and letterhead papers by printing such official documents on special papers with unique signs, logo or marks that cannot be easily forged. In addition, the findings of this study present positive implication in that administrative officers in COEs and other educational institutions can maintain confidentiality of digital information of their institutions by using cryptographic tools such as: block cyphers, string cyphers, and public key encryption.

The study found that the logical environment security control mechanisms identified in this study were not highly embraced by the administrative officers in COEs in South-South, Nigeria. By inference therefore, the result of the study showed that the level at which the administrative officers embraced the control measure was at the moderate level. Some of the logical environmental security control mechanisms 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 control; 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 control responsibilities; specify appropriate objectives to support effective environmental control mechanisms; 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. The findings of the study were in line with Abanyam et. al. (2020) who projected that compliance with control activities such as the 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.

Though this study has established that adoption of the information and communication, and logic al security control mechanisms are the keys to the survival of any institutions, yet there are some limitations of this study. First, the researchers used administrative officers in COEs in South-South Nigeria only. This has placed a limitation on 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 placed a limitation to 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.

5. Conclusion

This study investigated the control mechanisms embraced 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 mechanisms 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 clearly established in this study that effective information management through the information and communication, and logical environment security control mechanisms is the keys to the survival of the institutions from the unscrupulous hackers. Diligent application of the identified control mechanisms will also help the administrative officers 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 control mechanisms are effectively implemented. It is therefore, imperative for the stakeholders of COEs in Nigeria to take seriously issues of adaptation of control mechanisms for effective information management of in the institutions. Based on the findings of this study, the following recommendations were made:

1. Administrators and managements of COEs in Nigeria should enact effective policies and laws that support the adaptation of procedural preventive control mechanisms in their institutions.

2. The management of COEs should provide 21st-century ICT equipment that has updated applications that guarantee detective control mechanisms.
3. Administrators and Heads of Information Departments should organize regular staff trainings to help and upskill the administrative officers on the effective application of Information and communication control mechanisms and the skills required for its effectiveness operation.
4. The administrative unit heads of the COEs should organize trainings for the administrative officers on how to apply logical environment security control mechanisms to guarantee an effective network of information security of the institutions.
5. 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 control mechanisms.

References

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

Abanyamm, F. E. & Abanyam, V. A. (2021). Green Marketing in South-South 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

Acharya, R., Vityanathan, V. & Pether, R.(2009). Wireless LAN Security – Challages and Solutions. International Journal of Computer and Electrical Engineering, 1 (3). 45-63. https://doi.org/10.7763/IJCEE.2009.V1.39

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

Agomuo, E. E. (2014). Modern Office Technology: Issues, Procedures and Practice. Nsukka: Debees Printing Services.

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

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). http://dx.doi.org/10.12944/JBSFM.04.01.13

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/administrative-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 .

https://doi.org/10.52970/grsse.v2i2.183

Website: https://goldenratio.id/index.php/grsse/index ISSN [Online] 27975827

Lucey, T. (2005). Management Information Systems. Singapore: Seng Lee Press.

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 controls: The key to accountability. Retrieved on November 21, 2019 from: http://www.ucop.edu/riskmgt/ erm/documents/ pwc_int_ctrls.pdf.

McCrindell, J. Q. (2015), Framework for financial management and control. Journal of Finance Management Institute, 16(2) pp, 11-39. http://dx.doi.org/10.20431/2349-0349.0703001

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 control vs. application control. Prezi. Retrieved on September 8, 2019 from: https://prezi.com/iacknmfi6oxg/general-control-vs-application-control/

Hester W. J. Meyer (2003) Information use in rural development, The New Review of Information Behaviour Research, 4:1, 109-125. https://doi.org/10.1080/14716310310001631471

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 .

National Commission for Colleges of Education (2019). Nigeria Certificate in Education Minimum Standards for General Education Courses, TETF project 2012. Garki Abuja: Department of Academic Programmes.

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

Osuala, E. C. & Okeke, A. U. (2006). Administrative 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 control in New York State government. Retrieved on November 21, 2019 from: https://osc.state.ny.us/agencies/ ictf/docs/intcontrol_stds.pdf.

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

Techopedia (2019). Information management (IM). Retrieved on June 12, 2019 from: https://www.techopedia.com/definition/20012/information-management-im

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

University of California, (2017). Understanding internal controls. Retrieved on September 3, 2019 from: http://www.universityofcaliforna.com