International Journal of Library and Information Technology (IJLIT), Vol.7, June 2024. Pg.37 – 48

RISK MANAGEMENT OF DIGITAL INFORMATION IN OPEN DISTANCE LEARNING PROGRAMME: A CASE STUDY OF NATIONAL OPEN UNIVERSITY OF NIGERIA, ABUJA

YAHAYA MUHAMMAD SULAIMAN
Principal Librarian,
University Library,
Abubakar Tafawa Balewa University, Bauchi
E- mail: yahyabako95@mail.com

Abstract
Risk management in information digital information in distance learning programme is considered in this paper. The significance of NOUN as an open distance learning based higher education institution is pointed out. Threats and risks related to digital information resources were discussed and the significance of risk management in organizations is pointed out, with reference to the National Open University of Nigeria (NOUN). The study adopts a purely qualitative method using a purposive approach. Data was collected through interviews with the 6 targeted respondents. The study has sought to examine whether the institution has a well-laid enterprise risk management set out. Judging from the findings, ICT specialists among the personnel possessed competencies required in ICT risk management as well as proper maintenance of the ICT facilities. The assessment revealed that risk identification carries out to identify threats to digital information resources indicated that the risk is at low levels. Also, necessary measures are swiftly taken on threats identified due to risk assessment. Therefore, in most cases, the risks are at the tolerant level. To guard against any form of threats, the interviewees responded that risk management framework and strategies have been put in place. The study recommends that NOUN should intensify efforts in updating software, enlightenment on IT policies and understanding legal obligations on risk management. Personnel training on the diversity and complexity of cyber threats and related IT crime should also be a high priority of the institution.
Keywords: National Open University of Nigeria (NOUN), Open and distance learning (ODL) risk management, Digital Information Resources

Introduction

The rapid advancement of information and communication technologies (ICT) has revolutionized educational systems worldwide, leading to the proliferation of Open Distance Learning (ODL) programs. ODL programs, which provide flexible learning opportunities to a diverse range of students, often rely heavily on digital platforms for the dissemination of educational content, communication between students and instructors, and the management of academic records. The National Open University of Nigeria (NOUN), Abuja, as the foremost institution offering ODL in Nigeria, has embraced these digital innovations to cater to the growing demand for higher education. However, the increasing reliance on digital information systems introduces significant risks that, if not adequately managed, could compromise the integrity, confidentiality, and availability of critical educational data.

In the perspective of ODL, digital information encompasses a wide array of resources, including e-learning materials, student records, administrative documents, and communication logs. The management of these resources involves ensuring that they are protected from unauthorized access, corruption, loss, and other forms of cyber threats. Risk management, therefore, becomes a crucial aspect of maintaining the operational effectiveness and trustworthiness of digital information systems within the ODL framework. This is particularly important for NOUN, given its extensive network of students spread across various geographical regions, who depend on the reliability of these digital platforms for their academic success.

Despite the clear importance of risk management in digital information systems, many educational institutions, including NOUN, face challenges in implementing comprehensive risk management strategies. These challenges may stem from limited resources, inadequate training of staff, and the rapidly evolving nature of cyber threats. Additionally, the open and distributed nature of ODL programs adds another layer of complexity to managing risks effectively, as students and faculty often access digital resources from various locations and devices, increasing the potential for security breaches and data loss.

The case of NOUN presents a unique opportunity to explore the specific risks associated with digital information management in ODL and the measures that can be implemented to mitigate these risks. Understanding these risks and the current state of risk management practices at NOUN can provide valuable insights for other institutions with similar educational models. Moreover, it highlights the need for continuous improvement in the development and enforcement of policies, procedures, and technologies designed to safeguard digital information within the ODL environment.

In light of these considerations, this study aims to investigate the risk management practices of digital information in the National Open University of Nigeria's Open Distance Learning program. The focus will be on identifying the potential risks, assessing the effectiveness of existing risk management strategies, and proposing recommendations for enhancing the security and reliability of digital information systems at NOUN. The findings of this study are expected to contribute to the broader discourse on digital information security in ODL programs and provide practical solutions for improving risk management in similar educational settings.

It is a common saying that Information Communication Technology has revolutionized almost every human activity including the activities in the higher institution, where the transition from print to electronic information access continues to unfold. Therefore, the steady growth of digital information collections as major components of administration, learning, teaching and research has significant implications for higher institutions of learning and research libraries. Many institutions have been creating and collecting digital information produced in a wide variety of standard and proprietary formats, including common image formats, word processing, spreadsheet, and database documents. There is inferred assumption that institutions and their libraries will preserve the electronic information they create or the information that is entrusted to their care. To preserve this information, institutions must manage collections consistently and decisively. It is important to decide what should be preserved, in what priority, and with what techniques. Unfortunately, there is little guidance on where risk-management efforts should be directed.
In this digital era, as organizations use Information Communication Technology (ICT) systems to process their information for better support of their missions, risk management plays a critical role in protecting their information assets, from ICT-related risk. An effective risk management process is an important component of successful risk management for digital information resources and IT security programmes in general. The principal goal of an organization's risk management process should be to protect the organization and its ability to perform its mission. Thus, managers are encouraged to view operations from the perspective of an opponent to protect sensitive information from being loosed, corrupted, or falling into the wrong hands. Therefore, the risk management process should not be treated as a technical function to be carried out by only the IT experts who operate and manage the IT system. it should also be viewed as an essential management function of the organization considering its importance (Stoneburner, Goguen, & Feringa, 2002, Kalu & Igwe 2021). One of the major tasks of organizations' management is to protect their resources (both print and non-prints) to avoid damage, theft, alteration, diversion or attack of any nature. Hence, the security of organizations' digital information resources revolves around the security policy, access control mechanism, and breach detection structures, among other measures applied to protect the information from potential danger, threats or risks. Kalu and Igwe (2021) and Nkata U. Kalu (2021) highlighted the importance of risk management to safeguard critical information in learning institutions such as research data, personal information of scholars, staff, students, and sensitive information including the following:

1. It helps organizations safeguard their most sensitive information and data to prevent them from getting into the wrong hands.

2. It offers a different manner of approaching cybersecurity and information security by encouraging IT and security teams to look at their systems and processes from the perspective of potential attackers.
3. It also helps stop the inadvertent leak or exposure of sensitive data and improves organizations' security defenses.
4. By better securing the IT systems that store, process, or transmit organizational information
5. By enabling management to make well-informed risk management decisions to justify the expenditures that are part of an IT budget

This implies that organizations apply risk management to enhance their operations, hence the fundamental reason why digital information security is a major concern for organizations, especially academic institutions. National Open University of Nigeria (NOUN) as an academic institution has acquired and produced information resources in printed and digital format of administrative and academic values, which involves a lot of human and financial resources commitment that should be preserved. Besides that, gathering and organizing the information resources is tasking and laborious. Therefore, NOUN is supposed to pay attention to securing its resources and minimizing or mitigating information risks. Taking the value of information and Knowledge into account in the 21st century. Considering the numerous advantages of ICT-based services, the business, and academic world among other sectors are increasingly embracing digital technology in their activities, despite the risks associated with it. As such, several strategies or measures are deployed by academic institutions to secure or mitigate the risks of digital information loss. Fruhlinger (2020), felt securing information is very important and for information to be secured, a set of practices intended to keep data secured from unauthorized access or alteration, both when it is being stored and when it's being transmitted from one machine or physical location to another is put in place. In other words, the Concept of Information Security can be seen as freedom from attack and potential harm from others. Information security has therefore become the process or measure of protection against unauthorized access and use of information or data whether in print or electronic format.

ICT facilities and information resources in digital format risk assessment informs management's decisions about how to deploy risk responses toward information systems that could support NOUN objectives, it is therefore important that the management and other critical stakeholders drive the risk assessment process to identify what must be protected in alignment with the NOUN objectives.

Statement of the problem

Rapid evolution in information technology and the adoption of technology by organizations facilitate the achievement of their goals and objectives. However, threats related to digital information can come from outside the organization as well as from within the organization and can be a risk due to the presence of some weaknesses. ODL collections which support the users' community through access to its collections remotely are broad and varied. Information or data in digital format repeatedly travels from one computer to another and from network to network exposing the contents to numerous threats and interference such as technical and human errors, hacking, password theft, malicious code usage, and staff dishonesty among other threats. In a related study by Wessels and Sadler (2015) on information security, they revealed that cyber threat activity increases in occurrence, complexity, and destructiveness, thus organizations face a greater risk to achieving their strategy and objectives as a result of environmental, human and technical factors.

Consequently, there is a need to examine risk management incorporated into the NOUN operational system to identify potential sources that may pose a threat to the information systems of the institution. NOUN must mitigate major threats related to certain cyber incidents that could be harmful to the institution's electronic information resources and underlying data that is critical for learning, management and strategic decision-making.

Objectives of the paper:

1. To determine the level of the personnel competencies in ICT risk management and security
2. identify the threats that pose risks to the institution's information system
3. find out whether NOUN has a well-laid enterprise process for analyzing risk related to digital information resources

4. find out losses incurred as a result of threats or attack incidents on the IT facilities and the consequences.
5. find out the countermeasures instituted to mitigate or prevent risks based on information obtained and existing measures to protect the ICT systems from attacks

Methodology

The study adopts a purely qualitative method using a purposive approach. This approach was chosen to allow the researcher to gather in-depth information from the sample and obtain the best information to achieve the study's objectives. Moreover, the approach was chosen because it is the most prominent approach used in previous related studies. To determine the ideal respondents, the researcher focused on the research objectives. Thus, the respondents were purposively chosen for this study comprised of Senior management personnel who make decisions about IT security, Information system security officers who are responsible for IT security and Technical support personnel who manage and administer security for the IT systems, at the NOUN Headquarters Abuja, being the target audience due to their direct involvement with the subject matter (managing the server, acquiring, organizing, disseminating and preserving the information resources in electronic format) about which the researcher will be posing the questions.

Theoretical Framework

Specifically, there are abundant theories involved in Information Management (IM) and Information System (IS) research and it is unrealistic to incorporate all the theories. Therefore, the study is supported by 2 important theories in IM and IS, the theory on information security and the Illusion of Control theory. The theory of information security was formulated by Gregor (2006). The theory of information security originates from the area of information systems, built entirely from concepts that relate to the information and the breadth of systems that it can reside on. It applies to different levels, including strategies to protect information used by individuals, groups, and organizations and also protects information shared between organizations.

In this theory on information security, a statement on the modal qualifiers used to describe the relationship between controls and threats is: Some information is protected by some controls to produce all resources. This statement implies that if the information resources have not been protected by a control, then it cannot be considered a resource. Another is that all information to be used for organizational purposes is to be protected.

The illusion of Control Theory (ICT): The theory of IC refers to people often overestimating their control ability because of contextual factors or individual factors, resulting in lower risk perception or higher expectations of success probability. Existing literature review and meta-analysis have revealed several antecedents of IC, such as external incentives, involvement, skill estimation, and background factors. Moreover, the effect size of the sequence of the expected stimuli and reinforcement was strongest, which makes individuals mistakenly think that there is a connection between their behavior and results.

The Concept of National Open University of Nigeria: An Open Distance Learning (ODL) Institution

The developments in the field of informatics and technology today are reflected in the education system. Technologies play increasing roles as tools used in teaching processes in open and distance education systems. Distance education is a smart, contemporary and innovative education system that is completely independent of time and space, without the obligation of the student and the faculty member to come to the campus. Distance education is not a second-class education system applied to formal education. On the contrary, it is a state-of-the-art education system that has been applied in advanced developed countries for years and uses the latest measurement and evaluation methods. In Ogunode and Ayoko's (2023) view, distance education has become an important policy option for educational planners in developing countries. According to the authors, in the context of Nigeria, the increasing population, the growing national demand for education, dwindling financial resources, and increasing fiscal constraints, are the major factors narrowing access to education, thus leading to the establishment of Open and Distance Learning in Nigeria to salvage the promise of education. Commonwealth of Learning (2020) defined Open and Distance Learning (ODL) as the provision of distance education opportunities in ways that seek to mitigate or remove

barriers to access, such as finances, prior learning, age, social, work or family commitments, disability, incarceration or other such barriers. It enables students living in remote or isolated parts, or who are employees in full-time jobs or suffer from some physical handicaps to carry on their education at remote locations.

The National Open University of Nigeria ratified and signed into Law by President Shehu Shagari in 1983. Unfortunately, the Federal Military Government that succeeded the civilian government of Alhaji Shehu Shagari suspended the operation of the National Open University on 25th April 1984. However, in 2002, the suspended National Open University was reactivated by Chief Olusegun Obasanjo (NOUN, 2022). The National Open University of Nigeria is among the universities in Nigeria licensed to provide higher education on the premise of teaching, research and community service. National Open University is an organized higher institution, saddled with the responsibility of providing tertiary education through a distance learning model in Nigeria. As mentioned above, NOUN was established because the carrying capacity of face-to-face conventional tertiary institutions in Nigeria was insufficient. For instance, the Joint Admission and Matriculation Board (JAMB) received more than 1.5 million applications to Nigerian universities in 2022. Despite the total number of universities in the country having increased to 222 as of March 2023, the admission crisis persists in Nigeria, because their facilities could not allow admission of more than 20% of this number (National Universities Commission 2023). On the contrary, there is no carrying capacity set for NOUN's upper-limit admission. Thus, it is the country's largest tertiary institution in terms of student numbers, and it operates from the administrative headquarters in Abuja, Nigeria, with numerous study Centers spread throughout the country.

In striving to meet the one million-enrollment target for students set by the Federal Government, currently NOUN has over 600,000 students enrolled, the highest enrollment in West Africa become and a leading ODL institution in Africa providing functional, flexible, accessible and cost-effective education for all who seek knowledge in different courses. It currently has 104 centers spread nationwide even though only 150,000 students are active (Okebukola 2023). As a faithful representative of the Nigerian people, NOUN makes great use of Information and Communication Technology (ICT) to deliver an education tailored towards the globalized economy. The University offers exceptional academic programmes that meet the specific needs of all sectors of the global economy, in the Arts; Health; Law; Physical, Social, Agricultural and Management Sciences. NOUN is committed to openness and publishes many of its instructional materials as open courseware on its Web site (see http://www.nou.edu.ng /noun/NOUN OCL/courses.htm). NOUN students are instructed by open and distance learning methods within an open learning environment. This instructional mode is designed to provide students with the opportunity to acquire knowledge, skills, and techniques that may be relevant to either their present work situation or to future career prospects. Each course has materials written specifically for it, which students are expected to study before being examined. With the advancement in ICT, these materials written as lecture units or practical units, which students depend mostly on, are made available to students in digital format. among other benefits, students could work from anywhere, at their own pace, in their own time – with interactive online learning materials hosted on the NOUN virtual learning environment, (Okonkwo, 2012 &NOUN, 2022).

like other public universities in Nigeria, NOUN is faced with lots of challenges. It is evident that as an open distance learning higher education institution the medium of transmitting instructional materials largely depends on ICT, and emphasis on risk and risk management seems to be very imperative. It is the view of that, the paper is to critically assess the risk management of NOUN. In addition, the article is thus to contribute to the scholarly literature on risk management within higher education by reporting on a qualitative assessment of the appropriateness of the risk management framework of NOUN.

Potential Factors that result in Threats and Risks to Digital Information

In today's technology age, individuals started to live most of their lives in electronic environments. Individuals, governments, public institutions, social platforms, private companies and educational institutions started to communicate through virtual media Hillson, 2017). In line with this, technology risks, security vulnerabilities or errors in information systems that lead to serious business crises and loss are noticeable and considered as important threats worthy of concern. Threats can come from outside the

organization as well as from within the organization. In the absence of any weakness, the source of the threat is not a risk.

Specifically, a threat to information materials in any organization, is any circumstance, person(s), or events that threaten the safety and security of information materials. The level of vulnerability of the information often corresponds with the degree of threat realizable to it. For instance, Dawar (2016) maintains that in system and network security, threats remain present but are mitigated through the proper use of security features and procedures. Mitigation is any effort to prevent the threat from having a negative impact, or to limit the damage where total prevention is not possible, or to improve the speed or effectiveness of the recovery efforts.

Thus, knowledge of the step to identify potential sources, whether circumstances, person(s), or events that may pose a threat to information systems is very important to every organization. Taking the aspect of open and distance education programmes into account, Wallander and Keohane, (2002) and the State of Queensland (2023) identified the following as the most obvious sources of threat:

- Environmental (flood, lightning, storm, earthquake, fire etc.)
- Human errors (writing passwords on paper, accidentally deleting files, incorrect data processing, or careless data disposal etc.)
- Technical errors (hardware failures, short circuits, hard disk failure and lack of technological infrastructure etc.)
- Criminal IT threats (ransomware, hacking, fraud, password theft, malicious code usage, denial-of-service, security breaches among other staff dishonesty.
- Other factors that resulted in risks comprise of poor content quality, Malware, viruses, spam, scams, and phishing, deficiencies in organizational structure, where responsibilities are not fully defined, and communication gaps.

Certainly, these threats constitute risks of variant level to organizations' digital information, bearing in mind its disposable negative impact of a vulnerability, the probability and the impact of occurrence. In many organizational settings and personnel attitudes to words risk, having some highly valuable digital information resources being exposed to some kind of threats and danger cannot be ruled out. Moreover, we cannot stop the natural disaster from happening, the least we could do is, prepare to face them properly with lesser damage (Dawar, 2016). Therefore, without any deliberate steps to secure them, the resources are vulnerable to unwanted access, mishandling, pilfering and even to intruders.

Risk is regarded as naturally inherent in every human activity. The term risk is often used in different contexts that has a variety of meanings in business and everyday life. At its most general level, risk is used to describe any situation where there is uncertainty about what outcome will occur. Benjamin and Finaritra (2020) defined risk as a danger, a more or less probable inconvenience to which one is exposed or a possibility of an event that may cause damage. A potential to be vulnerable to harmful activity and further indicated that threats, weaknesses, effects and probability are components of risk. It is the element, factor or course of uncertainty as to damage, loss or danger. Risk involves opportunity, danger and uncertainty in which opportunity refers to using risks in favor of someone or something, the danger is the risk emerging from the events and uncertainty means risk arising from change. In other words, risk is the element of harm that one wants to avoid. It expresses uncertainty, suspicion, probability of loss and it refers to the possibility of damaging the system by taking advantage of a certain weakness of the system. An expectation of loss is expressed in terms of the likelihood that a particular threat will exploit a particular vulnerability with a (harmful) result in terms of impact on the business or mission. The impact may be expressed in terms of cost, loss of business/mission effectiveness, loss of life, etc (Ukoha & Igwe, 2021).

All businesses face risks regardless of the size of operations, location, types of products produced or services rendered to the public. It is instructive to note that unmitigated risks can spell enormous consequences such as the collapse of operations, failure and financial losses. Thus, companies and organizations need to stay aware of current risks, trends, and influencers in the technological environment. Based on responses to Committee of Sponsoring Organizations of the Treadway Commission (2019) survey on cyber security, (95%) of companies' executives surveyed admitted that their companies have experienced a wide range of cyber-attacks, with serious effects on their revenue, reputations, and leadership stability. Additionally, 90%

of organizations experienced at least one disclosure of sensitive production data within the past year while 41% experienced more than 5 instances. This is obvious because human beings particularly investors and managers have different attitudes towards risk. These diverse postures towards risks by managers and investors and other stakeholders alike are hastened by the nature of risks, which involves their unpredictability generally, and the inherent consequences or outcomes therein whenever they occur. The diversity of attitudes of business-minded people gives rise to various classes of people based on their peculiar attitudes to risks. Wessels & Sadler, (2015) are of the view that risk should be treated as a reality within institutions or enterprises as being something that "impacts an institution's ability to meet its objectives," because all kinds of organizations, regardless of their status, must face risk. Therefore, the need for developing ways to handle it through effective risk management procedures cannot be exaggerated, especially in keeping information away from internal and external threats.

The Risk Management processes in a Digital Information Environment

Risk management is the management in which necessary steps are satisfied, reviewed and reported to identify and evaluate the risks and put them at a reasonable level are done. Mohammad (2020) defined risk management as 'the act of evaluating and forecasting financial risks. The process also entails the identification of procedures to minimize the impacts.' On the other hand, the author termed risk management in information technology as the application of financial risks and the identification of procedures to reduce losses in the information technology field. Risk management encompasses a different number of processes depending on how the processes are broken down. For instance, a study by Stoneburner, et al, (2002) presented a risk assessment methodology that encompasses nine primary steps of identifying and controlling threats to an IT system. In related studies, Ruzic-dimitrijevic, et al, 2014; Zhang, 2020 and Mahmood (2020) categorized five steps in their work titled 'The risk assessment processes of higher education institutions' and 'operations security process to protect critical information respectively.' expressing that it is possible to perform information systems risk management with five basic functions, each of which has different importance but affects and supports each other: Risk Identification, Risk analysis, Risk assessment, Risk intervention, Monitoring risk management. What is important is that a risk management format should be able to safeguard the resources.

While organizations apply risk management to enhance their operations, Stoneburner, et al, (2002) enumerated some of the importance to include risk management help to contribute to the improvement of the performance of the administrations and their units and to make them more effective in achieving the key results targeted. Risk management helps to increase the continuity and quality of the services provided. Risk management helps reduces potential losses. Elaborating on the recognition attached to risk management internationally, Wessels and Sadler (2015) reported that several standard-setting agencies for enterprise risk management such as the Committee of Sponsoring Organizations (also known as COSO), the Australia/New Zealand Standard for Risk Management, the Combined Code and Turnbull Guidance, the Risk Management Standard by the Federation of European Risk Management Associations (FERMA) among others have emerged. Moreover, the authors stressed that the concept of risk management thus needs to be understood within the context of the provision of open distance learning by a higher education institution. Bearing in mind the rapidly changing environment within which this mode of learning is provided.

Unfortunately, studies have indicated that many organizations do not spend enough time gaining an understanding of what information systems are truly critical to the organization, in addition to having difficulty understanding where and how the information is stored and safeguarded. This can lead to attempts to protect everything, which may result in overprotecting certain information systems and under protecting others. because of this, placing a value on information systems and information risk management requires a high degree of collaboration between the administration and IT specialists as stakeholders. Besides, because many organizations are not able to act on all risks, given the limited time, budget, and resources available, management should also determine the levels of risk tolerance acceptable to the organization and focus its efforts to protect the most critical information systems. Therefore, risk management in the context of this study encompasses System Characterization, Risk / Vulnerability Identification, Risk analysis, Risk assessment and Risk intervention.

Process of Risk Management
The management of risk involves a process that is indicative of the fact such a task is normally taken by corporate entities in a well-defined manner to ensure that the result is in their best interest.. The section below, therefore, discuss the necessary process of risk management in respect of digital information resources, as rightly covered in this study.

Step 1: System Characterization
In assessing risks for an IT system, the first step is to define the scope of the effort. In this step, the boundaries of the IT system are identified, along with the resources and the information that constitute the system. Characterizing an IT system establishes the scope of the risk assessment effort, delineates the operational authorization boundaries, and provides information. The programme policies, standards, employee expectations, accountability, and all related communications should demonstrate support for the organization's core values and its risk management system. In other words, all the stakeholders' System security policies governing the IT system and the System security architecture are essential.

Step 2. Threat Identification
The goal of this step is to identify the potential threat sources and compile a threat statement listing potential threat sources that apply to the IT system being evaluated for the potential to cause harm to an IT system. The common threat sources can be natural, human, or environmental. In assessing threat sources, it is important to consider all potential threat sources that could cause harm to an IT system and its processing environment. In determining the likelihood of a threat, one must consider threat sources, and potential vulnerabilities.

Step 3: Vulnerability Identification
The analysis of the threat to an IT system must include an analysis of the vulnerabilities (A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised accidentally triggered or intentionally exploited and result in a security breach or a violation of the system's security policy), associated with the system environment. The goal of this step is to develop a list of system vulnerabilities (flaws or weaknesses) that could be exploited by the potential threat sources. Recommended methods for identifying system vulnerabilities are the use of vulnerability sources, the performance of system security testing, and the development of a security requirements checklist.

Step 4: Control Analysis
The goal of this step is to analyze the controls that have been implemented, or planned for implementation, by the organization to minimize or eliminate the likelihood (or probability) of a threat exercising a system vulnerability. To derive an overall likelihood rating that indicates the probability that a potential vulnerability may be exercised within the construct of the associated threat environment, the implementation of current or planned controls must be considered.

Step 5: risk Intervention
risk mitigation entails prioritization, analysis, and implementation of the most suitable risk control approach as per the risk assessment recommendations, to **s**ecure information from threats.

Securing Information from Threats
Generally, security involves safeguarding and prevention for safety. It can also be seen as freedom from attack and potential harm from others. Information security has therefore become the process or measure of protecting against unauthorized access and use of information or data whether in print or electronic format. The term 'information security' refers to the processes and methodologies which are designed and implemented in protecting print, electronic, or any other form of confidential, private and sensitive information or data from unauthorized access, use, misuse, disclosure, destruction, modification, or

disruption to provide integrity, confidentiality, and availability (CSRC 2019 & SANS, 2020). Thus, it is a central concern in organizations of all kinds.

It is imperative for organizations to take deliberate steps to secure all their printed and non-printed information resources. Without adequate efforts, techniques and tools to secure organizations and information resources, there would be loss, damage and destruction of valuable and highly prized materials. Organizations have suffered tremendous damage to their digital information resources. Therefore, it is necessary to examine all the implications of risk management in NOUN. It is important to note that adequate security measures to protect NOUN resources will enhance efficient service delivery. In today's world, information creation, use and dissemination have become a valuable asset. Therefore, the need to secure whatever valuable information in organizations' custody has become necessary and this has given rise to the concept of risk management. Consequently, the focus of this study will as well portray NOUN managers' diverse attitudes to risk management.

Data Collection Procedure and Analysis

Data on this study was collected through interviews, the development of which was informed by the objectives of the study. The researcher booked an appointment with the selected participants to gather data. All the 6 targeted respondents who participated in the study were interviewed over the telephone, giving a 100% response rate. Each respondent was interviewed for about 30 minutes. The interview exercise took 3 days. The respondents were assured of the confidentiality of the information they supplied.

Data Analysis

The qualitative data collected through the interview was analyzed thematically. The detail is contained in the following section.

Personnels' ICT Competencies

To achieve the objective, respondents were asked to comment on the level of the personnel competencies in ICT risk management and security. The results reveal that the organization delivers academic and administrative functions using ICTs. Therefore, the staff possessed the defined core IT competency required, including competencies in ICT risk management, as well as ICT facilities security management and maintenance. To be up to date, key function staff receive appropriate training on ICT risk management. Sequel to the skills acquired, the staff have competencies to understand risks associated with the institution's cyber, and evaluate the risks and address threats being faced by the cyber. This is an indication of the existence of good coordination among the stakeholders and a suitable characterization system. On whether the organization outsources IT services for critical activities in IT operations, sharing and protection, the respondents stated some years, these crucial tasks were outsourced. However, due to insincerity acts that led to loss of essential information and data, by the personnel engaged, their services were terminated.

Identification of IT risk

The next section of our interview focused on the identification of the IT risk process specific to the NOUN. According to the respondents, the organization had planned to carry out risks assessment and it does carry it out and already the staff were given training on risk management. That on regular bases, the organization carries out routine updates on its ICT facilities to identify possible risks. Procedures are always carried out to identify threats to digital information resources from environmental, organizational deficiencies, human errors, technical errors, or planned actions factors regularly. It was revealed that technical errors and criminal IT threats are the factors commonly identified at low levels.

Risk Assessment / Analysis

The interviewed persons reported that the organization has formally documented processes for analyzing risk related to digital information resources in place. In addition to that, the organization has a proactive system for analyzing its critical activities, and services, especially those related to information in digital format. Possible risks that could disrupt services concerning the academic and administrative progressions

are analyzed to determine flaws or weaknesses in the safety status of the system. Threats to digital information resources from all factors are assessed in terms of their consequences for the academic and administrative (including financial impact, the potential for academic disruption, the potential for administrative impact, and strategic impact). Notifications from detection systems are investigated on time and if the need arises and necessary measures are swiftly executed. Interestingly, the risks occasionally identified were very low and at the tolerant level.

Losses/corruption

On loss or corruption of vital information, the interviewees revealed that their organization recorded incidents of cyber threats and attacks, leading to loss of valid information and data caused by poor risk management. They explained that the incident occurred when the operation of the security of the system was outsourced. However, the interviewees revealed that the organization have not recorded cases of failed valid information submission, such as exams script, as a result of poor ICT skills or system failure.

Happily, the interviewees reported that at the moment, the levels of risk to the organization's digital information as negligeable, which does not hinder the services delivery to the clients. About area in which the organization is currently foreseeing the challenge arising from threats that could cause the severity of losses to digital information and service delivery. It was reported that there is none at the moment, as necessary measures were put in place to guard against threats from within, except for unavoidable human errors or technical errors. Furthermore, the respondents are in the know that criminal IT threats related to digital information can come from outside, likewise, natural disasters such as fire outbreaks or floods cannot be ruled out.

Risk Management Framework and Strategies

To guard against any form of threats, the interviewees responded that risk management framework and strategies have been put in place, as NOUN has an integrated and institution-risk management culture, based on a full and common understanding of the ICT risks it might face and how they are managed, which is conscious of risk tolerance level. In addition, the framework defines personnel roles and responsibilities in respect of the internal and external context for each risk assessment, the goal of the assessment, the criteria against which the risks are evaluated and the risk management objectives and benefits. These are communicated and embedded in all relevant parts of the organization. Interestingly, the respondents reported that NOUN management regularly intensifies efforts toward eradicating or minimizing risk or its prevention, along with formidable security measures.

Existing security measures

According to respondents, measures exist to protect the ICT systems from attacks either from the internet extranet or intranet include, including perimeter defense technologies like firewalls, IPS/IDS, web application firewalls, web filters, mail filters, antivirus, and content scanner devices (e.g. sandbox devices). Furthermore, appropriate procedures and security controls to protect the information while in transit through all types of communication facilities are taken, e.g. by using encryption technologies (applied either on the line or on the information itself). The interviewees also mentioned that the institution backs up its ICT systems in line with a predefined backup policy, taking into account the applicable essential digital information recovery requirements, and the cruciality of the underlying systems.

Conclusion

In conclusion, a study on risk management in NOUN headquarters as the largest open and distance learning systems in Nigeria can contribute to the challenge of developing quality higher education for all. The study has made it possible to analyze the risk management approach of the institution's existing protective strategies and proposed ways of reducing the risks inherent in ODL. The risk management project is already operational in NOUN on the System Characterization, Risk / Vulnerability Identification, Risk analysis, Risk assessment and Risk intervention. The results obtained showed that the risk level is at a tolerant level and is generally low, hence NOUN managerial efforts toward risk management is commendable. However, it must be admitted that efforts in updating software, enlightenment on IT policies and understanding legal

obligations for management risks need to be improved. For these unacceptable risks, preventive solutions that bring the risk back to the acceptance edge depend on the real implementation of the actions of students, teaching staff and administrative and technical personnel, as the main actors in the ODL. The management of risks related to ODL is, therefore, an area for discussion on the improvement of the training system in both developed and developing countries.

Recommendations

The following recommendations are provided to guide NOUN toward preventing or mitigating risks to digital information resources:

Depending on the sensitivity of the information to be accessed, the institution should properly control remote access and be subjected to strong authentication mechanisms. In addition to restricting access to its digital resources to only those users with access rights.

To ensure availability in case of disasters, backups should be stored at a different off-site location and sufficiently remote from the main one/primary hosting of the IT systems. And depending on the sensitivity of the information involved, backups should be encrypted to protect the information in case of loss or voluntary/accidental alteration.

updating software to the latest versions is necessary whereas backups should be regularly tested to ensure they are not corrupted. Do not download stuff randomly: Despite installing antivirus, it is wise to always verify every software you want to download to ascertain its origin. This is because some software are there to steal sensitive information from unsuspected downloaders.

Assigning a risk manager in each segment across the organization could prove beneficial. The manager can confer with other leaders and collaborate on pressing security issues. Because confining resources security solely to the IT department alone is not the best. Getting other departments involved is important in leveraging the resources you have internally.

Do not click on unknown links: Some unsubscribed or unknown emails are scams even though they look real. Hackers and attackers employ this style to have access to their victims' email or social networking accounts. Always check SSL information: To play safe while providing your personal or confidential information to a second party, make sure you are on an HTTPS link and not an HTTP link on some websites. These security layers ensure that all the information you provide will be encrypted on the website and no third party can access it.

For effective environmental and Disaster Control, providing a suitable and stable temperature, and disaster planning towards preventing and responding to damage from water, fire, or other emergencies should be a high priority of the institution.

Training staff in IT policies, procedures and understanding legal obligations for management risks should also be a high priority of the institution.

Reference

Benjamin, R.P. and Finaritra, R.M. (2020). The Management of risks related to the open and distance learning system. *International Journal of Engineering Technology Research & Management*. Vol-4 (10). (http://ijetrm.com/)

Committee of Sponsoring Organizations of the Treadway Commission (COSO) (2019). Managing cyber risk in a digital age. deloitte.com/us/about

Computer Security Resource Center (2019). Cybersecurity supply chain risk management. https://cserc.nist.rip/

Dawar, V. (2016) Digital information security for academic libraries. A paper presented at the Future Librarianship: Innovation for excellence.https://www.researchgate.net/publication /335389774 (8th November 2021)

Fruhlinger, J. (2020) Information security and practices. https://www.sans.org/information- security

Gabriel, D. (2023). The Sun Voice of the Nation Tuesday, April 25, 2023. https://sun newsonline.com/ open-university-targets-1m-students-enrollment/

Gupta, P. and Madusudhan, M (2018). Security of library materials: Challenges and solution. http://www.nedcc.org/resources/leaflets/3Emergencymanagement/11col lectionsSecurity.php

Kalu, N.U. Ukoha O. Igwe (2021). Preservation and security of library and information systems and resources. NOUN University Press National Open University of Nigeria Headquarters, University Village Plot 91, Cadastral Zone Nnamdi Azikiwe Expressway Jabi, Abuja

Mohmood, A (2020). Five-step operational security to protect your business.

Mosso, P (2020). Organizational security definition. https://orgsec.community/display/OS/ Organisational+security+definitions

National Universities Commission (2023). Monday Bulletin 6 March, Vol. 18 No. 08

NOUN (2022a) Nou.edu.ng/Vision and mission https://nou.edu.ng/vision- mission/ #:~:text=enhance%20Education%20For%20All%20and,flexible%2C%20but%2 0qualitative%20education%3B%20and

NOUN (2022b) Historical background of NOUN. https://nou.edu.ng/historical-background-of-noun/

Ogunode, N.J., Ayoko, V.O. (2023). National Open University of Nigeria: Contributions, challenges and way forward. *International Journal of Inclusive and Sustainable Education.* Vol.2(1) p128 https://inter-publishing.com/index.php/IJISE

Okonkwo, C.A. (2012). Assessment of challenges in developing self-instructional course materials at the National Open University of Nigeria. Vol 13 (2) 222 - 231

SANS (2006) Information security. https://www.sans.org/information-security/

Zhang, E. (2020). What is operational security? The five-step process, best practices, and more. https://www.digitalguardian.com

Mohammad, S. M. (2020). Risk management in information technology. *SSRN Electronic Journal*, https://doi.org/10.2139/ssrn.3625242

Nkata U. Kalu, U. O. I. (2021). Preservation and security of library and information systems and resources. National Open University of Nigeria, 1–46.

Ruzic-dimitrijevic, L., Dakic, J., & Sad, N. (2014). The risk management in higher education institutions, 2(1), 137–152.

Stoneburner, G., Goguen, A., & Feringa, A. (2002). Risk management guide for information technology systems recommendations of the National Institute of Standards and Technology.

Wessels, J. S., & Sadler, E. (2015). Risk management in higher education : An open distance learning perspective. Southern African Business Review Special Edition Accounting Research 2015, 74–98.