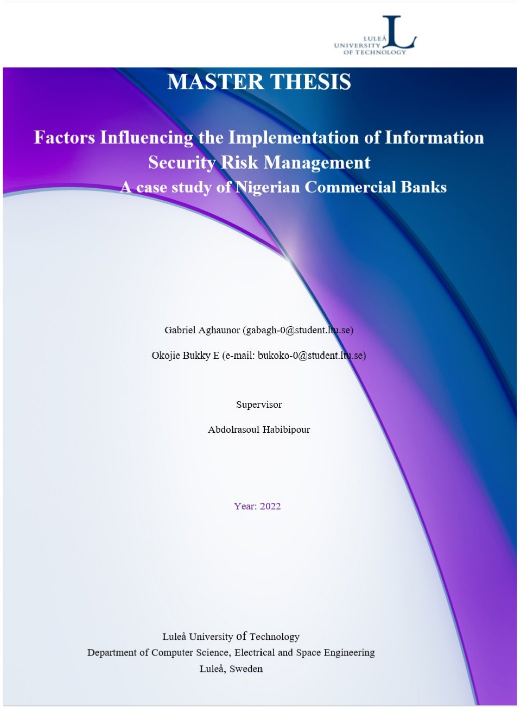
Factors Influencing the Implementation of Information Security Risk Management.

A case study of Nigerian Commercial Banks



MASTER THESIS

Factors Influencing the Implementation of Information Security Risk Management
A case study of Nigerian Commercial Banks

Gabriel Aghaunor (gabagh-0@student.ltu.se)

Okojie Bukky E (e-mail: bukoko-0@student.ltu.se)

Supervisor

Abdolrasoul Habibipour

Year: 2022

Luleå University of Technology
Department of Computer Science, Electrical and Space Engineering
Luleå, Sweden

Gabriel Aghaunor
Bukky Okojie E.

Information Security, master's level (120 credits)
2022

Luleå University of Technology
Department of Computer Science, Electrical and Space Engineering

ABSTRACT

The banking industry is one of the critical infrastructures in any economy. The services rendered by banks are systematically based on innovation, products, and technology to leverage their services. Several associated risks come along with the rendering of these banking services. The protection of critical information assets of any banking organization should be a top priority of the management. They must ensure that adequate provision is made to develop a strong strategy to control, reduce, and mitigate tasks, such as fraud, cyber-attacks, and other forms of cybersecurity exploitations.

Risk management is a series of actions to identify, assess and control threats and vulnerabilities in an organization's capital investment and revenue. These potential risks arise from diverse sources like credit risk, liquidity risk, financial uncertainties, legal actions, technology failures, business strategic management errors, accidental occurrences, and natural disasters.

This research study aimed to investigate the factors influencing the implementation of information security risk management in Nigerian Commercial Banks, using a social-technical system framework to address a fundamental human risk factor, which contributes predominately to the failure in information security risk management. This research was motivated by the fact that Nigerian banking sector is facing serious threats emanating from starting from cyber-attacks. This is evidenced by the ever-increasing cyber-attacks, as demonstrated by a total of 1,612 complaints from consumers of financial services over banking fraud and aggressive charges received between July and December 2018 of which 99.38% of these incidences were against the commercial banks. The banks are faced with a lot of vulnerabilities and cyber security threats, and most of the attacks that happened within the banking sector are focused on the customers, and employees through phishing and social engineering. These showed weaknesses in information security management within the Nigerian banking industry.

However, the study was guided by the social-technical theory that advocates for overall training to the stakeholders that helps in changing their beliefs and norms about organization of IS security. In order to find out the factors influencing the implementation of information security risks management in respect of Nigerian Commercial Banks, this study evaluated the influence of management support, technical experts support, funding and users’ security awareness to curb the cyber-attacks in Nigerian financial sector. The contribution of this research is expected to lead to the improvement in the financial system, and organizations, where cyber security and information security risk management processes are taken seriously, to reduce the high level of information security risk, threats, and vulnerabilities. Nigeria is a developing country, and at the same time fighting to develop a more conducive business investment environment to attract both national and international investors.

A mixed approach research (qualitative and quantitative) method was used to validate this research study. Data collection tools used included interviews and questionnaires. Data analysis was done using the SPSS and logistic regression model.

Keywords*: Information Security Risk Management System, Information Security Risk Assessment, Qualitative, Quantitative, Social technical framework User Security Awareness and Training, Management Support, Funding, Technical Experts' Support, Cyber Security, Banking, ATM.*

ACKNOWLEDGEMENT

First and foremost, we thank The Almighty God for the wisdom, strength, and knowledge given to us to go through this master’s program.

We thank the Management of the Lulea University of Technology for giving us the opportunity to realize our dreams by studying at this level. We thank and appreciate the entire staff of the Department of Computer science, Electrical and Space Engineering for their immense support and commitment to making us come out successful.

Our sincere gratitude goes to our supervisor Dr. Abdolrasoul Habibipour, for his intellectual support, corrections, and constructive comments during our thesis writing process.
Our profound appreciation goes to our families and relatives for their love, encouragement, care, and support all through.

Special thanks to the banks and especially the staff concerned for giving us the opportunity and sparing their time for the questionnaires and interviews.
We appreciate the moral support from friends, loved ones, and contributions from classmates.
Thank you all.

Gabriel Aghaunor and Bukky Okojie E.
June 2022
Luleå, Sweden.

Table of Contents

LIST OF FIGURES

LIST OF TABLES:

LIST OF ABBREVIATIONS AND ACRONYMS

ANOVA	-	Analysis of Variance
CBN	-	Central Bank of Nigeria
ICT	-	Information Communication Technology
IRC	-	Internet Relay Chat
IS	-	Information Security
ISPs	-	Information Security Policies
ISRAs	-	Information Security Risk Assessments
ISRM	-	Information Security Risk Management
NCPS	-	Nigerian National Cybersecurity Policy and Strategy
RM	-	Risk Management
SPSS	-	Statistical Package for the Social Sciences
TQM	-	Total Quality Management

1 Introduction

This chapter introduces the background of the study of information security risk assessment in relation to the factors influencing the implementation of information security risk management in Nigerian commercial banks. The chapter continues by introducing the statement of the problem, research questions that need to be answered, scope, and research purpose why this study. Following is the justification and the delimitations of this research study, and then concludes with the disposition and the structure of the thesis.

1.1 Background of the Study

Computer technology and information dissemination, cybersecurity attacks including hacking, and data theft are virtually pervasive in today's fast-paced technological age. Information security management is a way of safeguarding an organization's critical and sensitive data from being compromised through threats and vulnerabilities, for the purpose of maintaining integrity, availability, and confidentiality of data facilitating the controlled sharing of information while managing the associated risks in a dynamic threat environment (Chukwuma and Rai, 2010). Also, because of the high rate of electronic storage and transmission of information, the need for information security for persons and institutions has risen to high levels. Information security risk management in the context of the organization is explained as the protection of information, electronic data at rest or in transit, software applications, and hardware from unauthorized access. According to Lundgren and Möller (2019), data confidentiality, integrity, and availability are the primary goals of information security.

This research was motivated by the fact that public outcry over cyber-attacks has been on the increase in the Nigerian banking sector. For example, there were a total of 1,612 complaints from consumers of financial services concerning banking fraud and aggressive charges between July and December 2018; 99.38% of these were against the commercial banks (Nelson, 2019). This shows weaknesses in information security management within the banking industry. To identify and solve these problems, there is a need to research the factors influencing the implementation of information security risk management in the banking industry, particularly in Nigerian commercial banks, hence this thesis proposal. Several empirical studies have so far been conducted to identify factors influencing information security risks. For instance, a study by Glushenko (2017) observed that information security management is the process technology-dependent, and people-dependent, but less attention has been considered to people involved in information security (Glushenko 2017).

The study revealed critical factors affecting the efficiency of managing the risks of information security as management support (Arogundade et al., 2021). In the same breadth, Arbanas and Hrustek (2019) investigated key success factors of information systems security. The study summarized the most frequently cited key success factors of information systems security as management support, information security policy, information security education, training, and awareness. Another study by Semlambo, Mkude, and Lubua (2021) explored the factors affecting the security of information systems. The study results identified human factors, Unreliable information security policy, work environment, and demographic factors as factors affecting information security management. Human factor represents employees, management, and user and how they behave physically and psychologically in relation to organization IS security.

A study conducted by Wangen and Snekkenes (2013) indicated that the primary goal of Information Security (IS) is to protect the business from threats and ensure daily operational success by ensuring confidentiality, integrity, availability, and non-repudiation. The results of this study indicated that Information Security Risks management in an organization is made up of multifaceted processes which is influenced by a variety of factors such as technical expert support through education, training, and technology, all of which must be managed within a single framework.

A study conducted by Obeidat and Mughaid (2019), agreed that the budget is the major concern that affects the successful implementation of information security assessment. The budget is needed to buy the software tools for identifying the vulnerabilities and recommended controls, therefore, funding must be sufficient because without enough money organizations cannot be secured.

Another study conducted by Arogundade et al., (2021) on critical factors affecting the efficiency of information security risk management in the business organizations established that some of the known vital factors affecting the information security risk management are cost, organizational structure, organizational size, and philosophy of organization security which are all anchored on the funding. Zhi, Atif and Maynard (2018) did a study on the factors that influence security investments in SMES. The results of this study indicated that steps taken in ensuring that information assets are protected to the greatest extent possible or to an acceptable level. The prioritized list of scenarios authorizes security expenditure to be directed towards the highest risks (Zhi, Atif and Maynard, 2018). Gerber and von Solms (2005) as cited by Zhi, Atif and Maynard, (2018) posited that lack of or inadequate risk assessment shows that the organization has not utilized its resources to the fullest in addressing security risk and vulnerability exposures. Security of critical information can be accomplished through security awareness and training.

However, expanding the awareness can be implemented through training of employees to establish a sense of information security within the organization (Dhillon, 2017). A study conducted by Dhillon (2017) reiterated the need for organizations to have continuing education and training plans to accomplish the users' awareness that will aid the implementation of information security policies. A study by Fulford (2016) indicated that the human factor contributes mostly to security incidents in every organization as employees are the biggest threat to information security. The study further states that most of the security exploitation comes from the human error of omission, negligence, or intentional act which to some extent can be reduced by increasing users' awareness through training. Another study in the same vein conducted by Parsons, et al., (2010) observed that in every organization, employees are the greatest assets. Additionally, the study posited that a well-trained employee brings about efficiency in the information security system. Therefore, training programs are the basic rudiments for the information system security development process. When employees are trained properly in information security training programs, it helps to increase security awareness and productivity, which overall leads to reduced cost of security.

Based on the above studies, this current study therefore will explore the influence of management support, technical expert's support, funding, and users' security awareness on information security risks in Nigerian commercial banks. The study followed and was guided by socio-technical systems theory. The aim of this research is to articulate and evaluate the factors influencing the implementation of information security risk management in the commercial banking industry in Nigeria and to recommend a suitable way to control and mitigate the factor involved. It has been pointed out that the user of the applications possesses the weakest point in the security chain, due to their lack of awareness or negligence.

1.2 Statement of the Problem

A report released by the Central Bank of Nigeria (CBN) (2019) indicates that the situation in Nigeria, starting from public outcry over cyber-attacks, has remained on the increase. There were approximately 1,612 complaints from customers of financial services received between

July and December 2018 (Chijioke N, 2020). According to the Financial Security Report of the Central Bank of Nigeria (CBN, 2018), the statistics, indicated an increase of 173 complaints or 12.02 per cent over the 1,439 received in the first half of 2018; 602 or 99.38% of the total complaints were against commercial banks, while 10 complaints or 0.62% were against other Financial Institutions (Chijoke, 2020). During the yearly Bankers Committee retreat in 2019, in Ogun State, the Central Bank of Nigeria reported that cyber threat is more real than it used to be (CBN, 2019). According to a 2019 CBN report, bankers are now fully aware of the risks associated with their business as it relates to credit and operations but are slow in beefing up information security management. Cyber risk which is growing steadily in different parts of the world, calls for the banks, the CBN, and the government, to do something about it (CBN report, 2019). The CBN report (2019) advises the banks to do more in their management and control of cyber risks. The banks also need to invest more money in tools, whether software or hardware, that will help them in containing cyber risks in their operational environment. It is against this backdrop that this study seeks to find out the factors influencing information security risks assessment in Nigerian Commercial Banks.

1.3 Research Aim and Objectives

The purpose of this thesis is to explore and discuss the motivating factors influencing the implementation of information security risk management in the case of Nigerian Commercial Banks. The banking sector is always a prime target of attack by criminals online and offline. Developing countries are still struggling to attain the high level of information and cybersecurity as it is in the west.

According to Raytheon (2015), he stated that in a worse-case scenario, one single attack on a particular bank could result in a very big financial catastrophe to both the affected bank and their customers, as well as a country's financial systems in general.

The importance of implementing information security risk management in the selected banking sector cannot be over-emphasised. All stakeholders ought to be aware of cybersecurity trends and be vigilant within the domain. For example, a weak cybersecurity measures and control in the banking industry can expose customers critical information and compromise. Furthermore, Gupta, Chaturvedi, & Mehta, (2011) argued that when there is data breach, the cost of recovery in form of disaster recovery (DR) could be very expensive and time-consuming. Also, Dapp et al., (2014) observed that in our digital world today, there is a paradigm shift from traditional holding of cash to cashless transactions, meaning that enormous financial transactions are being done in a digital form. These trends according to Huyghue 2021, have increased more challenges in cybersecurity such as mobile devices and apps, weak credentials, lack of user security awareness, lack of budget and a heavy knowledge gap among the employees.

Considering the above, the following research questions are hereby proposed.

Research Questions

RQ1**:** To what extent does Management Support influence information security risks assessment in the case of Nigerian Commercial Banks? Technical Expert's support influence information security risks assessment in the case of Nigerian Commercial Banks?

RQ2**:** To what extent do Technical Expert's support influence information security risks assessment in the case of Nigerian Commercial Banks?

RQ3**:** To what extent does Funding influence information security risks assessment in the case of Nigerian Commercial Banks?

RQ4: To what extent does Users' Security Awareness influence information security risk assessment in the case of Nigerian Commercial Banks?

The influence of the management support of commercial banks was addressed in ***RQ1***. The factor can be statistically positively or negatively impacting the information security risk management, due to the mandate that is usually issued by the higher financial authority (CBN) in the country. The mandate usually stipulates the policies, control measures, and supervisory rules that commercial banks need to implement. Management decisions can have a great impact on organizational performance, and value creation for the shareholders (Gates et al., 2012; Chisasa and Young, 2013).

The influence of the technical expert's implementation of the risk assessment process was discussed in ***RQ2***. The evaluation and understanding of existing systems design and vulnerabilities associated with the potential benefits, costs and key performance indicators were measured to align with new controls. According to Torres et al. (2006 as cited by Yeo and Rahim 2016), human factor is the greatest risk involved in security issues. When technology have issues, it can easily be resolved, but humans are more vulnerable to attack (Westerman and Hunter, 2007). The socio-technical system approach should be incorporated into the information security risk management to help the management in controlling the risk involved. Discussion on ***RQ3*** was centred on the management's need to make adequate financial support or budgetary to facilitate the execution and implementation of information security risk management in the banking industry. If there is no adequate funding and integration of experts with technical know-how, the IS risk management implementation may fail.

In analysing the information security risk management, it is important to know that the user of the applications possesses the weakest point in the security chain, due to their lack of awareness or negligence, either knowingly or unknowingly. In ***RQ4**,* we discussed and highlighted that in every organization, employees are the greatest assets. A well-trained employee brings about efficiency in the information security system. Training programs are the basic rudiments for the information system security development process.

Banks are always a prime attack by criminals online or offline. Therefore, there is a need to address the areas where the weak link is visible, to secure a global financial chain that is interconnected. According to Raytheon (2015), he stated that in a worst-case scenario, one single attack on a particular bank could result in a very big financial catastrophe to both the affected bank and its customers, as well as a country's financial systems in general. The study was guided by socio-technical theory to address these complex and holistic security issues affecting the Nigerian commercial banking industry, and to recommend a suitable way to control and mitigate the factors involved.

1.4 Research Scope and Delimitation

The scope of the study refers to the parameters under which the overall study was carried out, meaning it specified what was covered, and how it is closely related to the framing of the research questions (Simon, & Goes 2013). The primary scope of this thesis is to investigate the factors influencing the implementation of information security risk management in Nigerian commercial banks. Although, there are multiple risks and challenges facing the banking sector, such as risks of granting loans and overdrafts to customers, project financing, management of debt, and so on. However, this study is only limited to information cybersecurity and the factors influencing the implementation.

The thesis deployed a framework of socio-technical systems theory to control information security risk management within the industry. Different constructs like management support, ISRM, and independent variables, such as technical experts, funding, and users' security awareness influence were discussed. A qualitative and quantitative approach to data collection was utilized before data analysis was performed.

The study's scope also entailed focusing on (10) ten commercial banks in Nigeria within the Southwestern States of Nigeria.

1.5 Justification for the Study

The following are the reasons for conducting a study on factors influencing the implementation of information security risk management in the case of Nigerian Commercial

Banks. First the reason for focusing the study to Nigeria as a country is because it is reported that cyber-attacks committed in Nigeria are more than any other country in Africa. A study conducted by Olusola et al, (2013) indicated that the world ranking in cyber-attack indicate that Nigeria is on top of the list after United States and Britain, but first in Sub-Saharan Africa (Chiroma et al, 2011). Nigeria is a developing country, and at the same time fighting to develop a more conducive business investment environment to attract both national and international investors.

Furthermore, a recent report by Deloitte (2021) ranked Nigeria 16th among the countries most affected by internet crime in the world in 2020, according to the Federal Bureau of Investigation (FBI) in its 2020 internet crime report (Deloitte, 2021). Documented cases of cyber-attacks most prevalent in Nigeria include yahoo attack, hacking, software piracy, pornography, credit card or ATM fraud, denial of service attack, internet relay chat (IRC) crime, virus dissemination, phishing, cyber plagiarism, spoofing, cyber stalking, cyber defamation, salami attack and cyber terrorism which mostly target financial institutions (Olusola et al, 2013).

Furthermore, one of the reasons for targeting commercial banks in Nigeria from a report by the Nigerian National Cybersecurity Policy and Strategy (NCPS) identifies the banking, finance, and insurance sector as one of its thirteen critical information infrastructure sectors heavily affected by cyber-attacks (NCPS, 2021). This is evidenced by findings in a study conducted by Nelson (2019) that indicated that a total of 1,612 complaints from consumers of financial services concerning banking fraud and aggressive charges between July and December 2018; 99.38% of these were against the commercial banks (Nelson, 2019). Therefore, it was imperative to perform an information risk assessment as it plays a critical role in prioritizing risks and securing IS data. Identifying the factors that hinders risk assessment therefore becomes paramount as the foundation for an effective risk management strategy. This study therefore identified four major factors that influence information risk management namely, management support, technical experts support, funding and users' security awareness on information security risks in Nigerian commercial Banks.

1.6 Significance of the Study

This study intends to be significant in various ways; it is believed that the findings of this study will be beneficial to IT practitioners and other organizations as it will provide IT practitioners and researchers with information on which to base sound decisions about the conditions that affect the implementation of Information Security Risk management initiatives in real-world settings. Also, the findings of this study would add valuable knowledge to scholars and academicians who may wish to use the findings of this study as the basis for further research on this subject.

1.7 Structure of the Thesis

This thesis is divided into six sections, and what is been discussed in each of the chapters are highlighted in this section.

- ***Chapter one*** introduces the overall paper, the background of the study, the statement of the problem, the research purpose and questions to be answered, the scope and limitations, justification, and the significance of the study.
- ***Chapter two*** discusses and evaluate the theoretical framework and literature review. Information security risk management concepts were highlighted, in relation to the socio-technical system theory. It further discussed the cybersecurity challenges facing Nigerian commercial banks, and how the risk assessment was measured in relation to the construct, dependent, and independent variables. The chapter concluded by mentioning the factors influencing the implementation of information security risk management in Nigerian commercial banks, followed by the overall summary of the theoretical framework.
- ***Chapter three*** revealed the research methodology philosophy, design, population of the study, and sampling design. It further highlighted the data collection method, data codification, methods, function analysis, and ethical considerations.
- ***Chapter four*** systematically present the empirical findings of the data collection of quantitative and qualitative mixed approach study from the questionnaires and interviews received from our respondents(interviewees). This will form the preamble for the data analysis and discussions.
- ***Chapter five*** presented the analytical section of the study where the information from the respondent was analysed scientifically, and data analysis and discussion, connecting it to the literature review was highlighted.
- ***Chapter six*** concluded the research paper, provides recommendations, lessons learned, and suggested ways for further studies.

2 Theoretical Background

This chapter reviews the theoretical framework and literature review related to information security risks management. The chapter begins with reviewing theoretical literature, then proceeded to discussing empirical literature on the factors influencing information security risks management. The literature review used a systematic method that entailed a preliminary search to identify relevant articles, ensure the validity of the proposed idea, avoid duplication of previously addressed questions, and assure that the study has enough articles for conducting its analysis. Moreover, the themes selected focused on relevant and important studies related to factors influencing the implementation of information security risk management. Therefore, while doing this step, the study conducted a systematic review and meta-analysis of determinant factors influencing the implementation of information security risk management. The inclusion and exclusion criteria were based on the research done on the relationship between the factors that influenced the implementation of information security risk management and the date the study was conducted. Inclusion criteria also included all the current studies conducted globally. The exclusion criteria entailed studies conducted in relation to the variables that influenced the implementation of information security risk management that were more than five years old.

2.1 Theoretical Framework

Semlambo, Mkude and Lubua (2021) observes that there are many theories that are proposed by various researchers in a pursuit of solutions for challenges that influence the security of information system (Kowalski, et al., 2018; Charitoudi and Blyth, 2013; Shahri and Mohanna, 2016; Han, Dai, Tianlin Han, and Dai, 2015; Lubua and Pretorius 2019).

Semlambo, Mkude, and Lubua (2021) further states that acknowledging different IS security theories and their contributions, helps in understanding the IS security literature and identifying factors that influence IS security in an organization and all factors identified in their study as the key factors in IS security. All these factors seem to have one common and very important attribute which is education, training, and knowledge. More so, the socio technical theory, distribute cognitive. theory and the general deterrence theory are the most frequently used IS security theories. Thus, this study proposed the solution of utilizing social technical theory by providing employees with appropriate training that will help in changing their beliefs and norms that can change their perception of organization IS security.

This theory examines human factors to be the essence in information security detection and prevention as currently information security is mostly perceived to be a technical issue (Zoto et al., 2018; Charitoudi and Blyth, 2013). Social technical theory is effective in moldering system security and its environment by examining culture, usability problem, security internal control and security requirement (Charitoudi and Blyth, 2013). Consequently, social technical theory can be used to analyse how people can be a contributing factor to IS security based on their perception and approach to organization IS security. Regarding the current study, the social technical theory seems to be more appropriate as lack of knowledge about information system security is a contributing factor to all other factors that affect the security of information system.

Semlambo, Mkude, and Lubua (2021) observes that adequate and regular training would assist in ensuring changes in employees' trust and sense of privacy about IS security. Knowledge about information security policy helps in ensuring these policies are being respected and adhered. Understanding how various work environment situations can affect information system security helps both managers and employees in securing IS security. Thus, understanding of all these factors and providing appropriate and regular trainings and awareness programs to both managers and users will help in strengthening organization IS security and get rid of security risk that keep on raging in organizations (Semlambo, Mkude and Lubua, 2021). Therefore, this theory is applicable to this study variables namely, management support, technical experts support, funding, and users' security awareness (Zoto et al., 2018).

2.1.1 Social Technical System Theory

The social-technical system theory states that when an organizational system is designed, it is imperative to consider both the social and technical aspect in the complex system as they are interdependent on one another. The social-technical perspective originates from pioneering work since in the 1960s, at the Tavistock institute and has been continued on a worldwide basis (Mumford, 2006). The elements that are incorporated in this theory consists of first the people, who have a common objective to achieve a goal. Secondly, the technology, which they use to operate in a physical infrastructure, processes, and share values culture and norms (Malatji, M., Von Solms, S & Marnewick, A., 2019). For the theory to be effective, they must be interactions, and interdependencies in all the sub-systems.

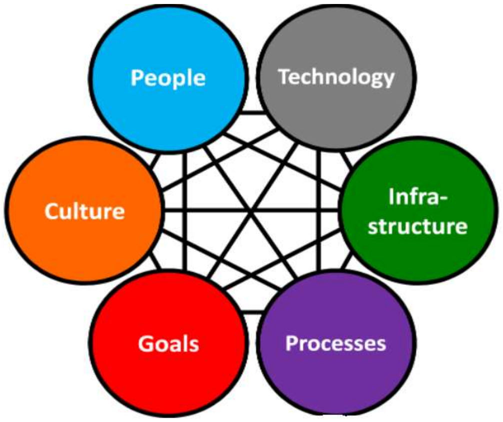


Figure 1: Hexagonal Socio-Technical Systems framework diagram (Adapted from Clegg 1979; Challenger et al. 2010; Davies et al. 2014).

The ecosystem of socio-technical system theory in figure 1 above, features the interdependencies of all the sub-systems, where there are integration and interactions within the organizational infrastructure. Relating the above theory to our study, some researchers have also incorporated the same theory in their research, in order to solve a common problem and understood how the socio-technical system could be deployed in an organization. Also, figure 2 below, shows the spherical structure of the socio-technical aspects and how they are embedded with each other but depicting different areas of operations.

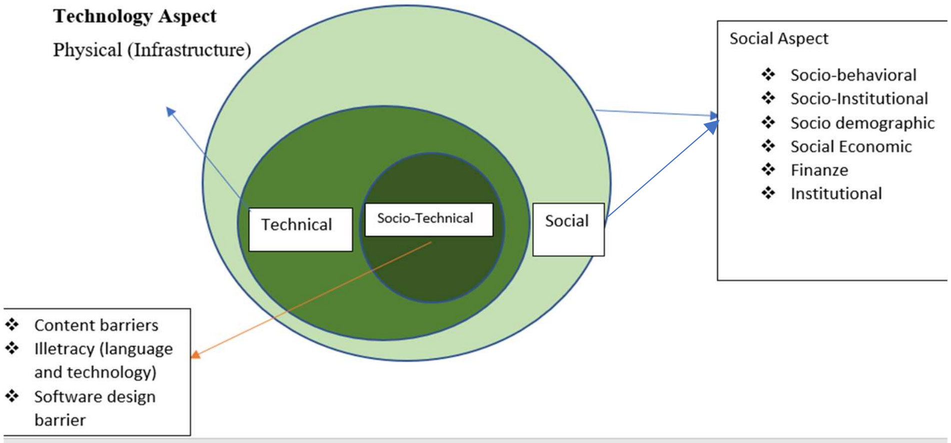


Figure 2: Social-Technical system framework depicting the technological and social aspect in a spherical diagram

2.2 Literature Review

Various studies by various researchers have explored the factors that affect information security risks management, and these are found various studies. This review will present studies that have sought to find out the influence of management support, technical experts support, funding and users' security awareness on information security risks management.

2.2.1 Management Support

Management support is essential and important in implementing the factors of information security risk management because, it reflects in assigning IT Security managers in the company to identify the importance of security in their organizations. A successful implementation of information security risk management factors needs very qualified staff. The Management tends not to start any procedure to guarantee the security of organizations because naturally they feel that the IT department is responsible for selecting the correct technologies, installing the essential software tools, keeping the technology in the organization and to protect the organization's information (Tryfonas, 2019). Therefore, the managements are in the position not only to identify business niches and opportunities but to make sufficient resources available for the implementation of ISM in the organization.

Alhogail, Mirza and Bakry (2015) worked on the comprehensive human factor framework for information security in organizations. The paper sought to bring together related human factors that have been identified in previous research into a logical, comprehensive framework. The framework was broken down into four diamond-shaped domains. Two domains are concerned with environmental and management issues, whereas the other two are concerned with preparedness and responsibility issues, representing an employee dimension. The domains at each of the diamond's four corners interact with one another, influencing human behaviour in terms of information security. A survey of experts' opinions on the framework was conducted to determine the importance of the framework's various components in human behaviour. The framework served as a foundation for future research into information security in organizations, as well as the development of controls for this purpose.

In a similar study, Alhogail, and Mirza (2014) carried out a study on framework of information security culture change. This paper examined the various change management models that have been used in the field of information security. The framework then combined a set of change management principles proposed from previous studies into a comprehensive multistep framework that supports and guides the transition in information security culture change within organizations. Furthermore, these principles serve as the foundation for developing an appropriate guideline to aid in the effective implementation of information security culture change. Information security professionals and academic researchers can use the framework to help them take proactive steps and measures to help change the culture.

In addition, a study by Glushenko (2017) observed that information security management is process dependent, technology dependent and people dependent, but less attention have been considered for people involved in information security (Glushenko 2017). This is probably due to the tendency to view the problem from the approach of the organization's requirement towards information security. Therefore, to handle these limitations, a questionnaire was constructed to gather information about factors influencing information security risk management from people directly and indirectly involved with organizational information structure. These factors were scrutinized and analysed with adjustable neuro-fuzzy inference system technique, machine learning method to reveal various critical factors affecting information security risk management. This approach revealed critical factors affecting the efficiency of managing the risks of information security as management support (Arogundade et al., 2021).

Arbanas and Hrustek (2019) investigated key success factors of information systems security. The study was based on a complete review of previous related study. The study therefore summarized the most frequently cited key success factors of information systems security identified in scientific articles indexed in relevant databases, with management support, information security policy, and information security education, training, and awareness ranking first, second, and third, respectively.

In the same vein, Semlambo, Mkude, and Lubua (2021) explored the factors affecting the security of information systems. This study discussed common factors affecting the security of information systems for modern computer users, including organizations and individuals, using a literature synthesis approach. The study results identified human factor, Unreliable information security policy, work environment and demographic factors as factors affecting information security management. According to a study conducted by Alhogail, Mirza, & Bakry (2015), human's factor represents employees, management, and user and how they behave physically and psychological in relation to organizations IS security. Regarding unreliability of security policies, the study stated that information security policy can be defined as roles and responsibilities of employees to protect information system and technological resources of their organizations. These policies are implemented to help employees to properly manage technological resources and managers of the organizations should help employee to follow these policies. Mostly, organizations adopt/creates IS security policies for the sake of compliance to international standards or governments, hence these policies fail to provide reliable security as they only remain in documents and not being practice. The management fails to enforce policies to users and provide them with appropriate knowledge and regular training to equip them with reliable tools and knowledge about organizations IS security. As a result, assisting in the saving of time and money by concentrating limited resources on elements that cause real concern in IS security (Semlambo, Mkude, and Lubua, 2021).

A study conducted by Obeidat and Mughaid (2019) identified several risks and threats exist in the operational environment of computers and networks that stems from inadequate management control, particularly where they can become exposed to security breaches. The study observed that there could be various reasons for the vulnerabilities, starting with an incorrect installation of systems and inaccurate usage or malicious software. Because of the quantity of personnel, packages and structures increase in the organizations, the control of the groups' information becomes more difficult and therefore vulnerability potential propagates. Considering preferable practice of hardware and software program, notwithstanding, encouraging, and empowering worker conduct, the organizations must make utilization of records and protection regulations through information security risks assessments (Obeidat and Mughaid, 2019).

Further findings of this study by Obeidat and Mughaid (2019) reported that one of the interviewees indicated that they are not allowed to do anything without permission from the management: the management need to give the employees support in implementing the security factors. Another expert said if the management does not understand the need to information security, then any attempt to prevent attacks and keep information safe will fail. Hone and Eloff (2017) clarified that the performance and the behaviour of employees towards information security becomes more coherent with secure behaviour if the top management shows concern about the organization information security. Thus, it is recommended that the security procedures are set by the attitudes of those at the topmost of the organization (Hinde, 2017).

2.2.2 Technical Experts Support

Yeo and Rahim (2016) states that the risk assessment team must have the expertise to apply the risk assessment methodology. Technical experts implement the risk assessment process based on the evaluation and understanding of existing systems designs and vulnerabilities associated with the potential benefits, costs and key performance indicator that realigned with new controls. According to Torres et al. (2006 as cited by Yeo and Rahim 2016), a critical success factor for ensuring security management of information systems is having honest, competent, smart, and skilful systems administrators.

A study conducted by Wangen and Snekkenes (2013) indicated that the primary goal of Information Security (IS) is to protect the business from threats and ensure daily operational success by ensuring confidentiality, integrity, availability, and non-repudiation. The author further stated that Information Security (IS) best practices rely heavily on well-functioning risk management (RM) processes, and RM is frequently regarded as the cornerstone of IS. Many public organizations rely on Information Security Risks management for them to be able to function optimally as information security management when it comes to organization, is made up of multifaceted processes which are influenced by a variety of factors such as the technical expert support through education, training, and technology, all of which must be managed within a single framework. According to Lundgren and Möller (2019), data confidentiality, integrity, and availability are the primary goals of information security.

2.2.3 Funding

All expert interviewees in a study conducted by Obeidat and Mughaid (2019), agreed that the budget is the major concern that affects the successful implementation of information security assessment. The budget is needed to buy the software tools for identifying the vulnerabilities and recommended controls, therefore, funding must be sufficient because without enough money organizations cannot be secured. Hinde (2017) defines budget as the financial facility which firstly estimates the costs and secondly measures the access required to the resources to reach a successful implementation of information security. Budgeting is dependent on the individuals' investments strategy that yields outcomes, but the impact of security investment depends not only on the investor’s own decisions but also on the decisions of other variables (Canavan, 2018).

One of the experts in the study conducted by Obeidat and Mughaid (2019), indicated that the vendors of security tools do not mention that after a while these tools must be updated to meet the new threats and attacks so without sufficient money the system organization becomes vulnerable to new attacks. It was, therefore, suggested that if organizations do not have the appropriate software or hardware tools, it would lead to difficulties in controlling some security concerns like access control tools, assisting employees to apply some security principles such as changing the password regularly or logging off after finishing their work. Another interviewee suggested that if they do not have the proper resources for implementing security measures, the goal of information security may not be feasibly clear to achieve within the organization.

A study conducted by Arogundade et al., (2021) on critical factors affecting the efficiency of information security risk management in business organization established that some of the known vital factors affecting the information security risk management are cost, organizational structure, organizational size, and philosophy of organization security which are all anchored on the funding. Organizational business practices have complementary support through information security risk management framework. Several organizations focus their attention of information security risk management efforts on the system of evaluation. Information security risk assessments (ISRAs) give organizations the ability of identifying crucial information assets and security risks (Werlinger et al. 2009).

Zhi, Atif and Maynard (2018) did a study on the factors that influence security investments in SMES. The study observed that information security risk management is a staged approach by which organizations can achieve a desired level of security. A risk assessment is aimed at identifying information assets that lies within the purview of an organization. Subsequently, threats and vulnerabilities are disclosed to develop scenarios that result in a breach of confidentiality, integrity, and availability.

Qualitative and quantitative methodologies were employed to estimate the probability of each scenario occurring and its associated impact (Gerber and Von Solm 2005 as cited by Zhi, Atif and Maynard, 2018). Subsequently, steps are taken for ensuring that information assets are protected to the greatest extent possible or to an acceptable level. The prioritized list of scenarios authorizes security expenditure to be directed towards the highest risks (that is, the scenarios with a moderately high impact and high probability). Organizations may control the risk by enforcing controls to prevent the potential breach from occurring (risk avoidance), reducing the impact after the breach has taken place (risk mitigation), doing nothing at all (risk acceptance) or placing the responsibility on an external party such as obtaining insurance (risk transfer) (Whitman and Mattord 2011 as cited by Zhi, Atif and Maynard, 2018).

Gerber and von Solms (2005) as cited by Zhi, Atif and Maynard, (2018) posited that lack of or inadequate risk assessment shows that the organization has not utilized its resources to the fullest in addressing security risk and vulnerability exposures. For example, should certain assets be not considered and reviewed in the risk assessment, then they may be unprotected. In the same way, if the estimation of probability and impact is inaccurate, not enough consideration has been given to security controls and protective strategy. Ultimately, vulnerability to information security risks can lead to adverse consequences for organizations, such as leakage of sensitive information and interruption or destruction of critical IT services. In the long run, the aim of risk management is to reduce the information security risk to an acceptable level in the organization (Gerber and von Solms 2005 as cited by Zhi, Atif and Maynard, 2018). Continuous performance of risk assessment in an organization allows for the application of systematic methods to identify security risks and guide them on the countermeasures and to defend their expenditure for security (Spinellis et al. 1999 as cited by Zhi, Atif and Maynard, 2018).

2.2.4 Users' Security Awareness

Regarding the users' security awareness, Dhillon (2017), posits that security of critical information can be accomplished through security awareness and training. However, expanding the awareness can be implemented through training of employees to establish a sense of information security within the organization (Dhillon, 2017). According to Dhillon (2017), organizations need to have continuing education and training plans to accomplish the essential outcome from the implementation of information security policies. The 2002 security awareness index report mentioned by ISO/IEC (2016) concluded that organizations all over the world are failing to make their employees aware of the security problems and concerns.

The human factor contributes mostly to the security incidents in every organization this assertion was supported the finding of Doherty and Fulford (2016) that employees are the biggest threat to information security. A use case of attacks through human factor is when employees themselves opened spam email or attached files. Majority of security exploitation comes from human error of omission, negligence, or intentional act. Therefore, human aspect needs to be seriously considered when it comes to information security. It is easily exploited and constantly overlooked. Companies spend millions of dollars on hardware, software, and security protection tools- firewalls, encryption mechanism, and secure access devices. It is almost money wasted because none of these measures address the weakest link in the security chain, where humans are the weakest link in the security chain. Therefore, if the security fails, that will weaken any organization (Anderson and Moore, 2018).

Some employees leave their computers on, other employees write the username and password on a small sheet near the computer, and this breaks the confidentiality to unauthorized people. That is why the research recommended doing a continuous course in training and awareness at all levels of the organization (Anderson and Moore, 2018).

Another study in the same vein conducted by Parsons, et al., (2010) observed that in every organization, employees are the greatest assets. However, the study posited that a well-trained employee brings about efficiency in the information security system. Therefore, training programs are the basic rudiments for information system security development process. When employees are trained properly in information security training programs, it helps to increase security awareness and productivity, which in overall leads to reduced cost of security. Greater participation in information security training programs is highly encouraged in all organization (Parsons, et al., 2010). The study recommended that information security training program should include regular evaluation and implementation of information technology based on the trends and changes. New challenges should be treated with the new technology. Therefore, the training awareness programs must be flexible to meet the new demand of the challenges. For this reason, IT experts should always attempt to develop themselves by attending various IT security awareness program to update themselves of the current issues in IT security measures. So, information security training programs are hereby considered in validating the model, and this hypothesis is proposed. Hypothesis 3 implies that there is a potential relationship between information security training programs and information security risk management (Parsons, et al., 2010).

Another study by Al-Omari, El-Gayar, and Deokar (2012) focused on user compliance with ICT policies to examine factors that affect IS security. The goal of the study was to produce a measurement tool that offers better measures for predicting and describing employees' compliance with information security policies (ISPs) by exploring the role of information security awareness in improving employees' compliance with ISPs. The study was the first to look at compliance intention from the viewpoint of users. In General, the investigation results show strong support for the proposed instrument and provide early confirmation of the validity of the underlying theoretical model.

2.3 The Concept of Information Security Risk Management

In the thought of Thorwat (2018), and Arbanas and Hrustek (2019), when the security of an organization's information systems is breached, such an organization faces risks such as data loss, cyber security attacks and business loss. Sahar, Al-Sarti and Abdul (2017) observed that Information Security Management Systems provide requirements for establishing, implementing, maintaining, and improving an information security management system. This adoption is a strategic decision for an organization that is influenced by the organization's needs and objectives, security requirements, and scaled based on the organization's needs. The information security management system entails applying a risk management process to protect the confidentiality, integrity, and availability of information. The components of an information security management system include Risk management based upon metrics of confidentiality, integrity, and availability; total quality management (TQM) applied based upon metrics of efficiency and effectiveness, a monitoring and reporting model based upon abstraction layers; a structured approach that contains people, process, and technology and finally an extensible framework from which to manage information security compliance (Sahar, Al- Sarti and Abdul, 2017).

According to Kuzminykh et al., (2021), information security risk management is a process that consists of identification, management and elimination or reduction of the likelihood of events that can negatively affect the assets of the information system, for the purpose of risk reduction that can potentially have the possibility to affect the information system (Kuzminykh et al., (2021). In the opinion of Peitier (2017), information security risk assessment consists of four distinct stages: asset identification, threat identification, vulnerability identification, and control identification and implementation. Information security risk assessment is an important part of organizational risk management practices that helps the organisation to identify, assess, and prioritize risks against criteria for risk acceptance and objectives relevant to the organization (Kuzminykh et al., (2021). Peitier (2017) identifies some factors that affect information security risk assessment such as management support; users' security awareness; technical experts and funding.

The ultimate target of information security policy is to provide confidentiality, availability, and integrity of information within any organization to eliminate cyber risks. The Institute of Risk Management (2018) defines cyber risk as any risk of financial loss, disruption, or damage to the reputation of an organization from a failure of its information technology systems. The possibility that an isolated cyber-attack could have consequences for the entire financial system is referred to as systemic risk (World Economic Forum, 2016). Every organization like the banking industry have their organizational aim, objectives, vision, and mission to make profit from their business. However, Nigerian commercial banks have been faced with cybersecurity challenges of how to secure its information from fraudsters, criminals, spamming as well as hackers to the information assets. For instance, according to Deloitte Nigeria, financial institutions, corporate businesses, state agencies and private individuals are increasingly being exposed to cyber-attacks and fraud through disinformation, impersonation, and other mechanisms such as phishing, which enables cybercriminals to access computers, mobile devices, and the intranet unnoticed to perform cyber- attacks from the inside (Ogbonnaya, 2020).

2.4 Information Security Risk Management Process

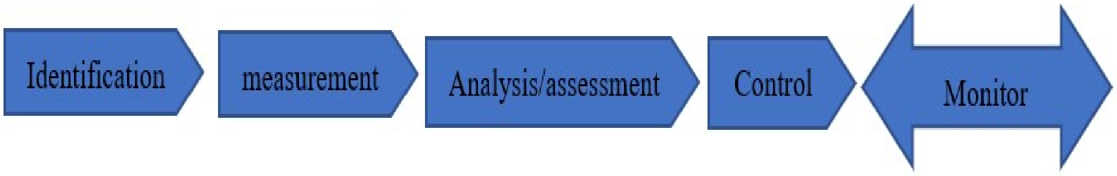


Figure 3: Information security risk management process (ISO 27001 Framework)

The above is the proposed information security risk management process in a nutshell. As the diagram in figure 3 stands, it sends a signal that before risk can be managed, it is very vital to be identified. As soon as the risk is identified, actions are taken to measure the intensity of the risk or to evaluate the result of the outcome.

Analysis/assessment process comes in to determine the consequences if any. Implementation of control measures are taken to avoid, reduce or transfer the risk depending on the magnitude or intensity. Thereafter, a monitoring steps are taken ascertain whether the expected process has been achieved (Bergström, Lundgren, & Ericson, 2019).

Before information risk management can be implemented, it must be identified first, because if there is no risk, there is nothing to measure, and nothing to value.

In the case of Nigerian commercial banks, cybersecurity risks need to be identified according to the threats and vulnerabilities the bank faces in their daily operations.

2.5 Cybersecurity Challenges (Risks) facing Nigerian Commercial Banks.

Information security risk can be analysed qualitatively in the case Nigerian commercial banks by considering the following cybersecurity challenges facing Nigerian commercial banks:

Ransomware: This type of attack happens when cybercriminals infect the system with a malicious file, that encrypts files/hard drive whereby users are logged out of their system, and eventually the criminals will start demanding a ransom (money), and in most cases, bitcoin from the innocent users before access to the files are given back to them (Wang, Nnaji, & Jung, (2020).

Social Engineering: Social engineering is one of the most powerful weapons used by cybercriminals on employees working in an organization. The reason is that people are the weakest and most vulnerable link in the chain of information security. Ugbe, (2021), stated that due to a lack of security awareness, people can be deceived in leaking some sensitive and critical information of their customers unknowingly. When it happens, it affects the bank employees and their customers, and even damage the reputation of the bank. Social engineering type of attacks can be in form of phishing, whaling, whereby emails with attachments claiming to be legitimate could be sent to massive receipts, but not knowing that it is a bait. It is imperative for all employees to be well informed about the security posture of the organization (Gaillard, A. 2021). Adequate provision of funds should be made available by the management to continuously train their staff as a going concern.

Need to secure cloud-base network: A lot of critical information and data of banks are being stored in the cloud infrastructure. Unfortunately, cybercriminal can still have access to compromise the data in the cloud. For this reason, it is important that banks should critically ensure that cloud infrastructure are well configured, do some configuration hardening to prevent any data breach.

This is where the influence of the technical experts comes into play. Well qualified cybersecurity expert services are highly needed to configure and implement the paradigm of security. In a more favorable case scenario, partnering with a third-party security consultants or company will enhance the security posture (Pramanik, et al., 2022).

The risk of remote workers: As stated by Omodunbi, B. A., et al. (2020), due to the covid-19 pandemic there has been a paradigm shift from the normal work force to remote (home office) or hybrid work force are ubiquitous. This have also increased cybersecurity challenges in the banking sector. Some employees no longer access sensitive data through a secure network with secured encryption channels, and some uses their organization's devices to access malicious website, thereby exposing the banks critical information to cybercriminal. For this reason, the influence of user's security awareness training will play a crucial role to keep implementing continuous security awareness training for all employees.

Attacks on supply chain: Cybercriminals always target third-party software vendors to the banks, by sending an advert with embedded malicious code to customers through their websites. This can be in form of product or request to update a software by entering the user's credentials Wright, et al., (2012). This can cause data breach and compromise the distribution systems and pave way for the cybercriminals to enter the customer's network.

Fraud using ATM Cards: There are instances where cybercriminals manipulate and clone ATM cards to steal money from the banking organization. In most case, the fraud perpetrators are insiders within the organizations (employees).

Sim card Manipulations. Most frequently, Nigerian commercial banks face losses of SIM card swap fraud by cybercrimes. A sim card swap fraud happens with a manipulation of carrier to switch a phone number which is possessed by a criminal, thereby diverting all SMS from a legitimate user to a criminal phone number. Again, there are insiders who organize these crimes with the ISP (Ugwuanyi, S et al. 2020).

2.6 Risk Assessment Measurement

Performing the quantitative research assessment before qualitative research, will help us to focus in the areas where we need to give priority in our information security risk management in the case of Nigerian commercial banks.

Empirically, the concept of information security risk management assessment in a research study is the abstract ideas or phenomena that were proposed to measure the risk factors (Gana, Abdulhamid, & Ojeniyi, 2019).

The identified variables from the RQs are the characteristics of the concepts, which were created by developing the construct from the theoretical framework. The variables were measured during the empirical observation stage of data collection from our respondents. The risk measurement and assessment follow immediately after the risk identification stage, to ascertain the overview of the nature and extent of the risks. Risk measurement is the evaluation of the result of the risks by using the set of risk factors that are valid during observation (Bouveret, 2018). To measure various risks, different techniques was applied such as nominal, ordinal, interval, or ratio. Furthermore, some sophisticated test was also carried out to determine the equality of variances, a group statistic test to determine the mean and standard deviation, and regression correlation test to determine the relationships between the dependent variable (DV), and independent variables (IV).

Basically, the risk assessment process is to determine which information asset is at risk and what threat could possibly cause a security breach.

According to Kuzminykh et al. (2021), for qualitative risk assessment, the focus is on the likelihood of an event rather than it's statistical probability.

These likelihoods are derived from analysing the threats and vulnerabilities, and then generating a qualitative or quantitative value for the critical asset or resources that may be affected (impact):

There are two widely used formulas for quantitative risk assessment supported by ISO/IEC 27005:2018 standard.

1. Risk = Threat × Vulnerability × Impact

where Threat × Vulnerability is likelihood.

2. Magnitude of Risk = Probability of event × Amount of damage

where the probability of event is calculated using this formula:

Probability of event = Probability of threat × Magnitude of vulnerability.

The severity of the impact, likelihood of occurring and controllability was used to determine the result. The result will assist the banks to proactively prepare themselves against the chances that the risk might occur or not. When it does occur, the severe impact it can have on the bank has to be managed by the disaster recovery (DR) team (Tooze, 2019).

Prioritization of risk in form of using risk analysis or risk evaluation is the main core of risk assessment measurement.

Risk analysis is based on the likelihood of occurrence and the consequences or impacts it will have. The likelihood depends on the probability that the risk will occur and how sporadically it will take place (Alali, M. et al. 2018). On the other hand, consequences can be measured by looking at the effects on the results of the outcome. If the frequency of occurrence of the risk and the effect it will have on the banks should occur, it will then give the banks the signal to know how important and valuable the risk stands. Risk evaluations were proposed and carried out before risk analysis is initiated. The risk evaluation process is usually done against an appropriate risk-acceptance criterion to give a qualitative ranking model. For example,

- High (meaning that it might be intolerable)
- Medium (it has a significant percentage of tolerance)

- Low (tolerable).

The above qualitative ranking approach will give a fair idea to the banks to determine how to make the right decisions.

2.7 Variables used to measure the above concepts

Measurement of variables can be in form of objective and subjective. For instance, the commercial banks performance in the areas of solving their cybersecurity risks can be objectively measured by the actual outcome of the policies they deployed. On the other hand, it could be subjectively measured based on opinion of the management. The management altitude towards solving the cybersecurity issues, would be measured by perception of how the organization adopt the policies and control mechanism.

The intention of the theoretical framework in this study is to extract the theoretical concepts relating to our topic, which we will utilise in conjunction with our empirical findings from our quantitative (deductive) and qualitative (inductive) mixed approach of data collection, to give us a fair and concise analysis, discussion, recommendation, and conclusion.

2.7.1 Dependent and Independent Variables

Therefore, the following variables from our research questions are hereby proposed to measure the concepts. It ranges from RQ1 to RQ4 which is the independent variables (IV), while the stage of information security risk management is the dependent variable (DV).

2.8 Factors Influencing the Implementation of ISRM in Nigerian Commercial Banks.

2.8.1 User Information security Awareness and Training

Security of critical information can be accomplished through security awareness and training. However, expanding the awareness can be implemented through training of employees to establish a sense of information security within the organization (Dhillon, 2017). According to Dhillon (2017), organizations need to have continuing education and training plans to accomplish the essential outcome from the implementation of information security policies. The 2002 security awareness index report mentioned by ISO/IEC (2016) concluded that organizations all over the world are failing to make their employees aware of the security problems and concerns.

In addition to, some employees leave their computers on, other employees write the username and password on a small sheet near the computer, and this breaks the confidentiality to unauthorized people. That is why the research recommended doing a continuous course in training and awareness at all levels of the organization (Anderson & Moore, 2018). Based on the above factor, it therefore means that information security awareness is considered to validate the model, because there is a potential relationship between Information security awareness and information security risk management.

2.8.2 Information Security Policy

Information Security Policy (ISP) is an important instrument used in ISM to demonstrate the need for and scope of information security (Prislan, Mihelič & Bernik, 2020). It highlights the procedures, policies, and structure to be followed in the organization. Basically, Information Security Policy (ISP) advocates top management's commitment towards protecting the critical information assets. There are many international standards like NIST, GDPR that states the prerequisite, procedures and controls that should be used in ISP. When we incorporate these standards, it gives Information Service Policy (ISP) another level of authority towards the success of ISM implementation. So, ISP is hereby considered to validate the model, because there is a potential relationship between Information Security Policy and Information security risk management.

2.8.3 Information Security Training Programs

In every organization, employees are the greatest assets. Subsequently, a well-trained employee brings about efficiency in the information security system. Training programs are the basic rudiments for information system security development process. When employees are trained properly in information security training programs, it helps to increase security awareness and productivity, which in overall leads to reduced cost of security. Greater participation in information security training programs is highly encouraged in all organization (Parsons, et al., 2010). Information security training program should include regular evaluation and implementation of information technology based on the trends and changes. New challenges should be treated with the new technology. Hence, the training programs must be flexible to meet the new demand of the challenges. For this reason, IT experts should always attend attempt to develop themselves by attending various IT security awareness program to update themselves of the current issues in IT security measures. So, information security training programs are hereby considered in validating the model, because there is a potential relationship between information security training programs and information security risk management.

2.8.4 Technical Experts' Support

Yeo & Rahim (2016) states that the risk assessment team must have the expertise to apply the risk assessment methodology. Technical experts implement the risk assessment process based on the evaluation and understanding of existing systems designs and vulnerabilities associated with the potential benefits, costs and key performance indicator that realigned with new controls. According to Torres et al. (2006 as cited by Yeo & Rahim 2016), a critical success factor for ensuring security management of information systems is having honest, competent, smart, and skilful systems administrators. So, IT security technical expert support is hereby considered in validating the model, because there is a potential relationship between IT security experts and information security risk management.

2.8.5 Motivation of Employees

There are different ways to motivate employees. For example, through promotion, salary increment, fringe benefits and host of others. Those are ways of rewarding the employees for a job well done in the organization. However, disciplinary actions again to be taking against any employee, whose conduct is not aligned to the organization. This is done to bring sanity to the organization. Most often, employees, being the end users of an information technology (IT) system, are sometimes unaware about the consequences of their action when using the devices. Some employees share the opinion that, IT is only responsible for the protection of organization critical information. But it is not true. Every employee has the obligations to protect information assets of their organization. There are repercussions of not fully involving in the protection of organization information (Liu, Wang & Liang, 2020). However, when employees are motivated through rewards or incentives, they would comply with organizational information security policy. Information security standards, internal risk control, government policy and regulations, preventing information threats and as well support the top management, hence an organization would be able to achieve its objective for better performance. Therefore, the motivation of employees was considered in validating the model, because there is a potential relationship between the motivation of employees and information security risk management.

2.8.6 Management Commitment and Support

Management commitment is essential in implementing the factors of information security risk management, it reflects in assigning IT managers in the organizations' department to identify the importance of security in their organizations. A successful implementation of information security risk management factors needs very qualified staff. The Management tends not to start any procedure to guarantee the security of organizations because naturally they feel that the IT department is responsible for selecting the correct technologies, installing the essential software tools, keeping the technology in the organization and to protect the organization's information (Tryfonas, 2019). Therefore, the managements are in the position not only to identify business niches and opportunities but to make sufficient resources available for the implementation of ISM in the organization.

In a study conducted by Obeidat & Mughaid (2019), one of the interviewees indicated that they are not allowed to do anything without permission from the management; the management need to give the employees support in implementing the security factors. Another expert said if the management does not understand the need to information security, then any attempt to prevent attacks and keep information safe will fail. Hone & Eloff (2017) clarified that the performance and the behaviour of employees towards information security becomes more coherent with secure behaviour if the top management shows concern about the organization information security. Thus, it is recommended that the security procedures are set by the attitudes of those at the topmost of the organization (Hinde, 2017).

Therefore, top management commitment was considered in validating the model, because there is strong and potential relationship between top management commitment and Information Security Risk Management.

2.8.7 Funding

All expert interviewees in a study conducted by Obeidat & Mughaid (2019), agreed that the budget is the major concern that affects the successful implementation of information security assessment. The budget is needed to buy the software tools for identifying the vulnerabilities and recommended controls, therefore, funding must be sufficient because without enough money organizations cannot be secured. Hinde (2017) defines budget as the financial facility which firstly estimates the costs and secondly measures the access required to the resources to reach a successful implementation of information security. Budgeting is dependent on the individuals' investments strategy that yields outcomes, but the impact of security investment depends not only on the investor’s own decisions but also on the decisions of other variables (Canavan, 2018).

One of the experts in the study conducted by Obeidat & Mughaid (2019), indicated that the vendors of security tools do not mention that after a while these tools must be updated to meet the new threats and attacks so without sufficient money the system in an organization becomes vulnerable to new attacks. It was, therefore, suggested that if organizations do not have the appropriate software or hardware tools, it would lead to difficulties in controlling some security concerns like access control tools, assisting employees to apply some security principles such as changing the password regularly, or logging off after finishing their work. Another interviewee suggested that if they do not have the proper resources for implementing security measures, the goal of information security may not be feasibly clear to achieve within the organization. This implies that there is a strong and potential relationship between Funding and Information Security Risk Management.

2.9 Summary of the Theoretical Framework.

The intention of the theoretical framework in literature review is to establish the gap found, and extract the theoretical concepts relating to our topic, which we utilised in conjunction with our empirical findings from our quantitative (deductive) and qualitative (inductive) mixed approach of data collection, to give us a fair and concise analysis, discussion, recommendation, and conclusion. It is imperative to mention that there were some gaps in the literature review, such as not having an adequate information from the population of the study, especially the top management of the banks. In Nigerian context, the area of information security risk management is under-developed, and for this reason, it calls for further studies in the future. Therefore, the variables from our research questions, and which were highlighted in the literature review, were used to measure the concepts. It ranges from RQ1 to RQ4 for the independent variables (IV), while the dependent variable (DV) is the stage of information security risk management.

3 Research Methodology

This chapter describes the research design, population of the study, sampling design, data collection method, types of data, tools, analysis, and instrument used in this study. The study used a mixed method usually a combination of both inductive and deductive approach. According to Creswell and Plano Clark (2017), deductive research works from the top-down, from a theory to hypotheses, to data, and to add to or contradict the theory. In contrast, they define the inductive researcher as someone who works from the bottom-up, using the participants' views to build broader themes and generate findings interconnecting the themes (Creswell and Plano Clark, 2007).

3.1 Research Philosophy and Positivistic Paradigm.

Cohen and Crabtree (2006) contend that research philosophy or paradigm is the underlying assumption upon which research and development in the field of inquiry is based. The proposed study will adopt the positivist research philosophy based on its relevance to proposed study. The study will use data gained from positive verification of observable experiences rather than introspection or intuition. In addition, the positivist approach tends to exclusively rely on theories that can be directly tested (Bhattacherjee, 2012). Studies by Cohen and Crabtree (2016) and Creswell (2003) assert that the positivist research approach belief on prediction and control. Such a study is embedded on cause and effect to be used as a basis for predicting and controlling natural phenomena and the goal to discover these phenomena. The advantage of this philosophy is that it forms the basis for empirical verification that a researcher could rely on observations or measurements of the phenomena to provide accurate data (Schiffman & Kanuk, 2017). In this study, therefore, objectivity was achieved as the method will allow statistical analysis to generate findings on the factors influencing information risks management.

3.2 Research Design

Research design according to researchers Deutch & Cook, (2017), is a framework for empirical research aimed at answering specific research questions, and testing hypotheses and must specify at least three processes: the data collection process, the instrumentation process, and the sampling process. Kothari (2011) argued that a research design is the arrangement of conditions for the collection and analysis of data in a manner that aims to combine relevance to the research purpose with economy in procedure.

Hence, this study used descriptive research. Ary (2018) describes descriptive research as scientific research that describes event, phenomena or fact systematically dealing with a certain area or populations. The main purpose of a descriptive survey is to detail the situation as is, that is, the researcher reports the findings (Kombo and Tromp 2011). The choice of the design is supported by Bickman, Rog, and Hedrick (1998) who stated that the descriptive approach is used when the researcher is attempting to answer what is or what was questions. A qualitative approach through a survey in form of questionnaires was used to collect data from the departmental staff managers using open-ended and close-ended questions.

A mixed-method- quantitative and qualitative techniques were used for the descriptive survey. The main rationales for undertaking a mixed method in this study are the fact that such an approach will aid in triangulation, completeness, offsetting weaknesses and providing stronger inferences and answering the research questions.

Regarding methodological triangulation approach, which refers to the use of more than one method for gathering data (Bekhet, & Zauszniewski; 2012). The data collected was analysed, by means of questionnaires, semi-structured interview and documentation, which allow for greater validity in a study by seeking corroboration between quantitative and qualitative data.

Regarding completeness, using a combination of research approaches provides a complete and more comprehensive picture of the study phenomenon (Hussein, 2009). In addition, a mixed-method helps in offsetting weaknesses and providing stronger inferences as many authors argue that utilizing a mixed-methods approach can allow for the limitations of each approach to be neutralized while strengths are built upon thereby providing stronger and more accurate inferences (Bryman, 2015).

Furthermore, a mixed method helps in answering different research questions. In support of this fact, Creswell and Plano Clark (2007), argued that mixed methods research helps answer the research questions that cannot be answered by quantitative method alone and provides a greater range of tools to meet the aims and objectives of a study. Furthermore, Sale, Lohfeld & Brazil (2017) identify how a combination of research approaches (inductive and deductive) are useful in areas such as social research because of the complex nature of phenomena and the range of perspectives that are required.

Moreover, merging qualitative and quantitative techniques also aid in showing the comparisons and variances amongst specific features of an occurrence (Bernardi, Kleim, and von der Lippe, 2014). The Likert scales were used to gather quantitative data whereas the open-ended questions and responses from the respondent were analysed qualitatively, meaning it was done in a descriptive and interview transcript format.

The justification for using a mixed approach (qualitative and quantitative) is that there is no possibility to quantify the answers derived from the open-ended questions that will come from the respondents of the targeted population. Quantitatively, variables can be numerically measured, qualitatively, construct like risk management needs to be measured using a key performance indicator (KPI), and interview with the respondents. It will therefore follow a descriptive form to analyse the factors, to help the management in making an informed decision. The quantitative approach was used to analyse the input for the close-ended questionnaires. For example, Yes/No answer, and the answers given by using a Likert scale of 1-5 where 5 = Strongly agree (SA), 4 = Agree (A), 3 = Neutral (N), 2 = Disagree (D), 1 = Strongly disagree (SD). With the use of SPSS coding, quantitative analysis can be done using the above numerical numbers.

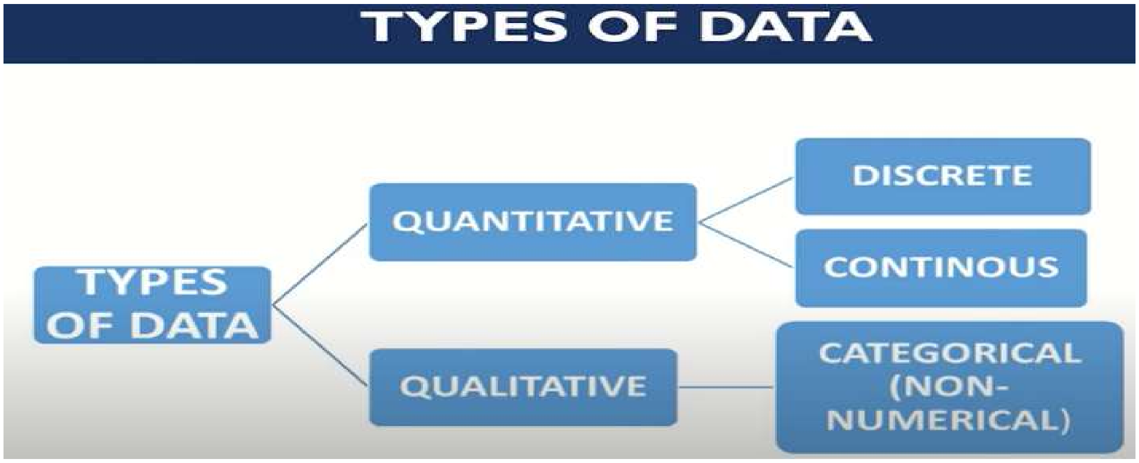


Figure 4: Types of data used.

In figure 4, the quantitative data are numerical and can be mathematically computed. There are divided into two categories. These are discrete data (a whole number of targeted populations in the study) and continuous data which was measured using interval and ration scale (Markon, Chmielewski, & Miller, 2011).

Qualitative data is categorical but not numerical in nature. It is rather a descriptive style of data collection, in form of interview transcripts, documentation and observations. Qualitative data can be measured further with a nominal value (for example, the gender of the respondent), or ordinal scale (for example, the qualifications of respondents).

3.3 Population of the Study

Population refers to the larger group from which the sample is taken (Kombo and Tromp, 2011). The target population of this study consists of 10 commercial banks out of the 22 commercial banks in Nigeria with emphasis on those within the three states of the Southwestern States of Nigeria. Out of the total number of the population stated above, the study will target five core departments namely: IT Security department, Operation's department, Internal control, and audit department, IT department, and risk management department. A mixed approach (inductive/deductive) in the form of a questionnaire/interview was used to collect data from the departmental staff managers using open-ended and close-ended questions.

3.4 Sampling Design

A sample is a defined role of a statistical population whose properties are studied to gain information about the whole (Webster, 1985). Sampling design refers to the method used to choose the sample from the population (Hubbard et.al., 2016).

The qualitative dimension of this study involved the adoption of a purposive sampling approach, which was used in selecting ten (10) management staff across the five major commercial banks in Nigeria. The selection includes two management staff selected from each of the banks representing the management team of the bank.

While the quantitative segment of this study used a stratified random sampling technique in selecting respondents for this study among the management team of the selected bank. The first strata include the selection of two upper-level management staff across the selected banks. The second strata involved a random selection of two middle-level management staff across the selected banks. While the third strata involved a random selection of two lower-level management staff across the ten (10) branches of selected banks, as a whole, sixty (60) management staff was randomly selected for this study.

3.5 Data Collection Method

Data collection is very vital in our research because the result of the study depended upon the data collected, and the method of data collection. It is a way of gathering, measuring and analysing data from the mixed approach (inductive/deductive) to help us answer our research question/problems or any proposed test hypothesis.

3.5.1 Qualitative Data

The qualitative data were collected through key informant interviews. The justification for adopting this approach is to elicit real-life data on customer's experiences relating to information risk management of their banks. Interview questions aligned with the following theme: banking experience frequency, online transaction support frequency, confidentiality level frequency of ATM card and pin, frequency of experiencing debit without successful transaction, and online transaction support frequency.

Thereafter, questions were asked concerning cybersecurity issues in the banks and how the risk of cyberattacks affects banks generally. Respondents from different bank gave their opinion at different levels. The next phase of the interview was the influence of management support, influence of technical support and user awareness training. Positive responses were received from different banks and all interview protocols and transcripts were duly documented under the analysis chapter.

3.5.2 Quantitative Data

Data collection was also done by administration of questionnaires and interview transcripts containing close-ended and open-ended questionnaires. A questionnaire is a research instrument consisting of a set of questions (items) intended to capture responses from respondents in a standardized manner (Bhattacherjee, 2012; Kothari, 2011).

The questionnaire was prepared thematically based on the research questions. The questionnaire for this study is divided into four sections where the first section contains questions relating to the general information of the respondents while the second to fifth section contains questions relating to the factors influencing information security risks assessment in Nigerian commercial banks.

The collection of data was done through both open-ended and closed-ended questions and documentation of researcher notes. This enabled the researchers to obtain relevant information, alongside data synthesizing and analysis, which was simultaneously performed. Through the analysis, the researchers, used the SPSS software to extract scientific code and information obtained through interviews and the development and verification of the data collected from the respondent. The questionnaire approach was aimed at knowing the points of view and the perceptions of the actors directly involved in the studied phenomenon.

The selection of participants for the interviews was determined by the level of their expertise within the core departments of the banks. For the coding procedures to work with good results, the researchers orientated themselves to compose sample according to the views obtained from the interviewed participants. The table 1 below show the data collection table for the research study.

Method	**Tools and Instrument**
Administration of Questionnaire	Questionnaire based on quantitative measurement
Interview/Documentation Analysis	Documentation analysis on qualitative measurement, where necessary observation can be included.

Table 1: Data collection table for the research study.

RQ Code	Research Questions	Type of variable/Construct	Indicators	Measurement scale	Method of data collection	Instrument /Data collection tools	Data analysis Techniques
RQ1	To what extent does Management Support influence ISRM assessment	-Management Commitment Independent variable	-Policy -Monitoring Control measures -Provision of Training and awareness to employees	KPI KPI	- Administering questionnaire -Interview transcripts	-Questionnaire -Interview guide	-Frequencies and percentages -Inductive Analysis (qualitative)
RQ2	To what extent does Technical Experts support influence ISRM assessment	-Network Infrastructure -security specialist Independent variable	-Implementation of security measures - Competencies of the Experts	-Ratio -Nominal -Nominal -Nominal	- Administering questionnaire -Interview transcripts	-Questionnaire -Interview guide	-Frequencies and percentages -Inductive Analysis (qualitative)
RQ3	To what extent does Funding influence ISRM assessment	-Budget Approval -Independent variable	-Monetary support	-Ratio -Nominal -Nominal -Nominal	- Administering questionnaire -Interview transcripts	-Questionnaire -Interview guide	-Frequencies and percentages -Inductive Analysis (qualitative)
RQ4	To what extent does Users' Security Awareness influence ISRM	-Training -Independent variable	- No of Trainings -Content of the Training module -Adequacy of materials -Technology	-Ratio -Nominal -Nominal -Nominal	- Administering questionnaire -Interview transcripts	-Questionnaire -Interview guide	-Frequencies and percentages -Inductive Analysis (qualitative)

Table 2: Data collection matrix table of questionnaire/interviews based on the variables for each concept/construct.

The table 2 above shows the data collection matrix table for the construct and the variables (***RQ1-RQ4***). it is imperative to mention that there is a difference between variable and construct.

"Management support", "Risk assessment", are an example of constructs, and these cannot numerically be measured on their own. It was measured through key performance indicators (KPI), like having interviews with the respondent/employees. However, variables were numerically measured, because they can be quantified in units.

3.6 Research Model

A mixed approach was deployed to analyse the data. Quantitative data from the questionnaires were computed and coded into the SPSS computer application for descriptive statistics. The collected data was sorted, classified, coded, and tabulated for ease of analysis according to the coding rules (Martin and Acuna, 2002).

The qualitative data from the semi-structured interview were analyzed using content analysis, where the content to analyse was based on our research questions. Qualitative content analysis is a research method for the subjective interpretation of the content of text data through the systematic classification process of coding and identifying themes and patterns (Elo, et.al. 2014). The process of qualitative content analysis in this study entailed; reading all data repeatedly to achieve immersion and obtain a sense of the whole. Then, data was read word by word to derive codes by first highlighting the exact words from the text that appear to capture key thoughts or concepts.

Next, the study approached the text by making notes of the first impressions, thoughts, and initial analysis. As this process continues, labels for codes emerge that are reflective of more than one key thought. These came directly from the text and then became the initial coding scheme. Codes were sorted into categories based on how different codes are related and linked. The result of the data computation was analysed, and a conclusion was drawn.

3.7 Data Analysis and Presentation

The data were sorted, categorized, and coded before being tabulated for analysis. The information was summarized and organized into themes. The SPSS (version 22) computer software was utilized to facilitate the study because it is more user-friendly and best suited for analyzing management-related attitudes (Martin and Acuna, 2002). NVIVO version 12 was used to analyze qualitative data using content analysis. While statistical products and services solutions (SPSS) were used to analyze the quantitative data, a multiple regression model was used to estimate the relative importance of each variable in relation to the factors that influence information security risk assessment in Nigerian commercial banks. The regression model formular used is as follows:

Y= ß0+ ß1, X1 + ß2, X2 + ß3,X3 + ß4,X4 + 0e

Where:

Y= Information Security Risks Assessment (Dependent Variable)

ß0= Constant

ß1, ß2, ß3 and ß4…… coefficients

X1= Management Support (Independent Variable)

X2= Technical Experts' support (Independent Variable)

X3= Funding (Independent Variable)

X4= Users' Security Awareness on information security risks (Independent Variable)

e = error term

Descriptive statistics such as mean, and variance and standard deviation was used to analyse the data. The results were then analysed and presented on frequency distribution absolute and relative (percentages) frequencies, measures of central tendency and dispersion (mean and standard deviation respectively), tables, pie charts and bar charts.

The other independent variables can be regarded as continuous variable which can be measured by a Likert scale between 1 to 5, where 1 = strongly disagree and 5 = strongly agree.

Data analysis was based on the number of the quantitative questionnaire and the interview (qualitative) questions that were administered. All these variables were determined by the scale of measurement.

Using the quantitative approach, the numerical data was analyzed using statistics, and the narrative data was analysed using inductive and thematic approach.

Statistics is a body of mathematical techniques or process for gathering, organizing, analysing, and interpreting numerical data (Best and Khan, 2009, p.354).

In the light of the above definition, we agreed and used two approaches:

1. Descriptive statistics: This involves using a designated number to represent a group of numbers or population.
2. Inferential statistics: In this case, we could make inferences and prediction of the targeted population based on the sample of the data that was collected. This takes the form of probability (that is to make inference), which might possibly lead to testing hypothesis if any. The table below illustrates the main methods we used to analyse and present our data.

Type of Statistics	Method of Analysis	Statistical Tool	Type of data
Descriptive Statistics	Graphical	Bar graph, Pie charts	Categorical
Descriptive	Tabular form	Histogram, Frequency distribution	Continuous Categorical
Descriptive	Numerical	Mean, Median, Range, standard deviation, and variance	Continuous
Inferential Statistics	Correlation	Pearson product, correlation coefficient	Continuous and Categorical
Inferential Statistics	Regression	Simple Linear Regression and multi linear regression	Continuous
Inferential Statistics	Test of Comparison	T-test and ANOVA	Continuous

Table 3: Data analysis method and techniques.

In presenting the data stated in table 3, we started from the descriptive statistics, highlighting the method of analysis, statistical tools, and type of data, before moving to the inferential statistics in that order. Thereafter, the data is presented, interpreted, and the discussion of the overall research findings.

3.8 Ethical Considerations

This study embraced research ethics by avoiding any form of harm, suffering, or violation of fundamental rights and privacy of respondents while developing and administering data collection tools and techniques.

Respondents were assured of anonymity and confidentiality. The identified participants were protected by neither giving their names when presenting research results nor including any personal details which may reveal their identity. The participants were not required to put their names in the interview protocol. Those who wish to do so were also welcomed. The study also seek consent from the respondents to participate in the study and those who could not participate were exempted from the study, and those who wish to withdraw from the study were also allowed to do so. Moreover, the information that was provided by the respondents as agreed was only used for academic purposes and the purpose of the study was hitherto explained to them in a language they understood well.

4 Result

This chapter presents the datasets and the results of the findings based on the qualitative and quantitative approach the was employed in the research study including demographics, the respondents' perception on the research questions raised and how these questions were answered with the data collected using frequency count and percentages.

4.1 Research Questionnaire Administration

Sixty questionnaires were sent out to the various respondent of the commercial banks that were chosen during the sampling selection of the population. The reason is to try and obtain adequate information for the data analysis. Out of forty questionnaires returned, twenty-five questionnaires representing 75% were reasonably good for use, while 15% of the questionnaires were rejected, due to incompleteness, and lack of proper input.

According to Nakpodia, Ayo and Adomi (2007), it was argued that in Nigeria, a response rate for a research survey is between 45% - 73%. However, a response rate of 30% is meant to be sufficient in a research survey based on the argument raised by Pielsticker, D. I., and Hiebl, M. R. (2020). Furthermore, for those questionnaires that were not responded to, they were discarded and not represented. A nonresponse factor bias was however calculated.

4.2 Background Statistics and Demographics

4.2.1 Respondents Percentage Distribution of Staff Cadre

Sequel to the descriptive statistics, the criteria we use in selecting the category of the respondents, revealed that, upper-level management was 5%, the middle-level management with 35% and the lower-level management has 60%. Most of the respondents were middle and lower-level managers.

However, it is assumed that most of the respondents within this category are employees working at the bank branches, and most of them were of officer's grade and lower-level managers who were probably the branch managers. It was a bit difficult getting access to the top-level manager like the members of the board. This was one of the challenges we faced in our research study.

4.2.2 Percentage Distribution of Departmental Staff

At the various departmental level of operation, IT department have 23%, risk management 17%, Audit/internal control have 25%, IT Security department has 24%, and lastly operation departments have 11%.

During the cause of the research, we discovered that some banks have the risk management department combined with internal control section, especially in the regional and branch level offices. During the research study, we were fortunate to come across one of the highest-level ranks of respondents, who happens to be a board committee representing one of the commercial banks.

With that statistic, we got at least 1% of respondent with a high degree of information that we required. The category of respondent with top classification of employees like officer's grade represents about 44%. These percentages can be assumed to relate to the obstacle in getting access to the top-level management in the banking sector.

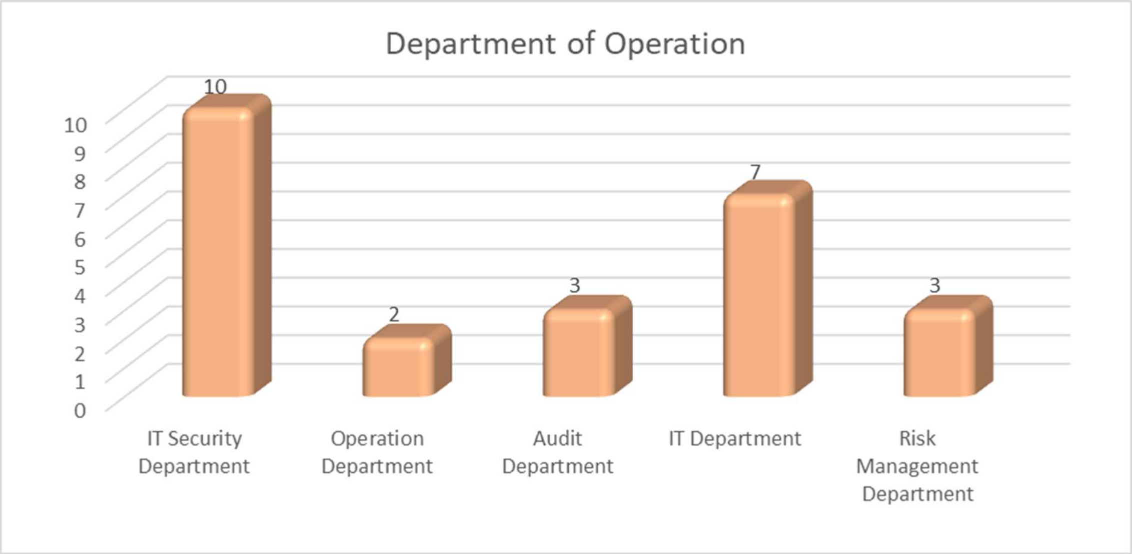


Figure 5: Percentage Distribution of Departmental Staff

4.2.3 Percentage Distribution of Working Experience

The branch level operational staff consists of supervisors' officers and managers. Digging deep into the preliminary analysis, it revealed that 35% of the respondents have working experience between 1-7 years, and 20% of the respondents have the working experience not less than ten years. It was therefore concluded that the selected population (respondents) have enough working experience in the banking industry to answer the interviews and research questionnaire without any serious bias.

4.2.4 Percentage Distribution of Gender

Out of fifty participants, 65% of the respondents were male while 35% respondents were female by implication majority of the respondents are male respectively as shown in the figure below:

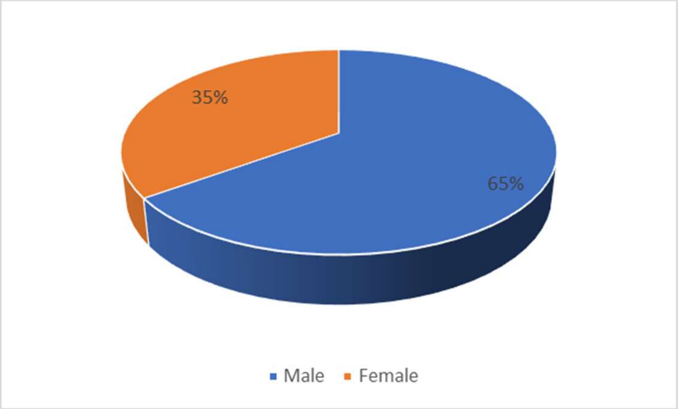


Figure 6: Percentage Distribution of Gender

These findings can be interpreted to mean that the two thirds gender rule is observed in the commercial banks under study.

4.2.5 Percentage Level of Education

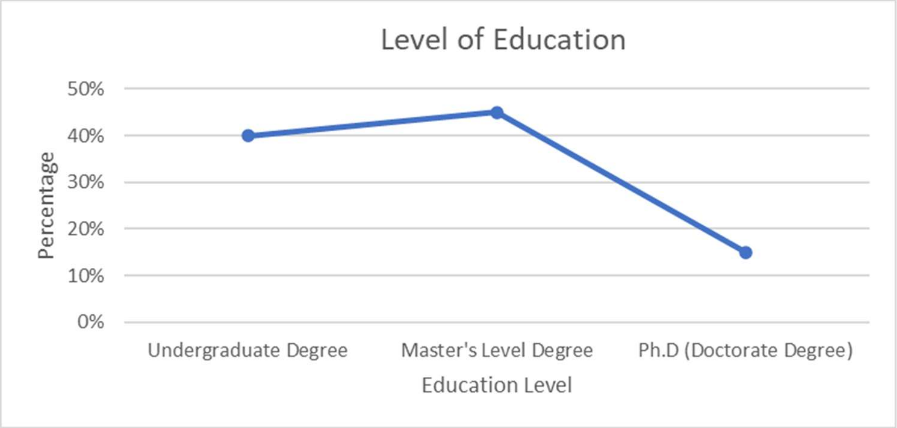


Figure 7: 4.2.4 Percentage Level of Education

The above figure 4.2.4 indicates 40% of the respondents had an undergraduate degree, 45% had a master's level degree while 15% of the respondents had a doctorate degree. These findings indicate a normal distribution which can be interpreted to mean that the employees in these commercial banks are well balanced.

4.3 Relationship between the Independent Variables and Dependent Variable

Zero-order summary showing the relationship between management support, experts' supports, funding, users' security awareness, and risk assessment among the banks in southwestern states in Nigeria.

Variables	**Mean**	**St.Dv**	**1**	**2**	**3**	**4**	**5**
Stage of Security Risk Assessment	24.01	6.43	1.00				
Management Support	37.53	5.77	0.452^{**}	1.00			
Experts' Supports	21.76	3.01	0.508^{**}	$.741^{**}$	1.00		
Funding	17.04	3.24	0.490^{**}	$.626^{**}$	$.718^{**}$	1.00	
Users' Security Awareness	17.500	3.06	0.250^{*}	$.794^{**}$	$.385^{**}$	$.497^{**}$	1.0

Table 4: Relationship between the IVs and DV

Table 4 reveals the relationship that exists between management support, experts' supports, funding, users' security awareness and risk assessment among the banks. Risk assessment positively correlated with emotional maturity (r=0.452, p<0.01), experts support (r=0.508, p<0.01), funding (r=-0.490, p<0.01), and security awareness (r=-0.250, p<0.01). This implies that increase in management support, experts' supports, funding, and users' security awareness will lead to an increase in risk assessment. Thus, a significant relationship exists between management support, experts' supports, funding, and users' security awareness and risk assessment.

4.4 Joint Contributions of the Variables on ISRM

The joint contributions of management support, experts' supports, funding, and users' security awareness on risk assessment is shown in the table 5 below.

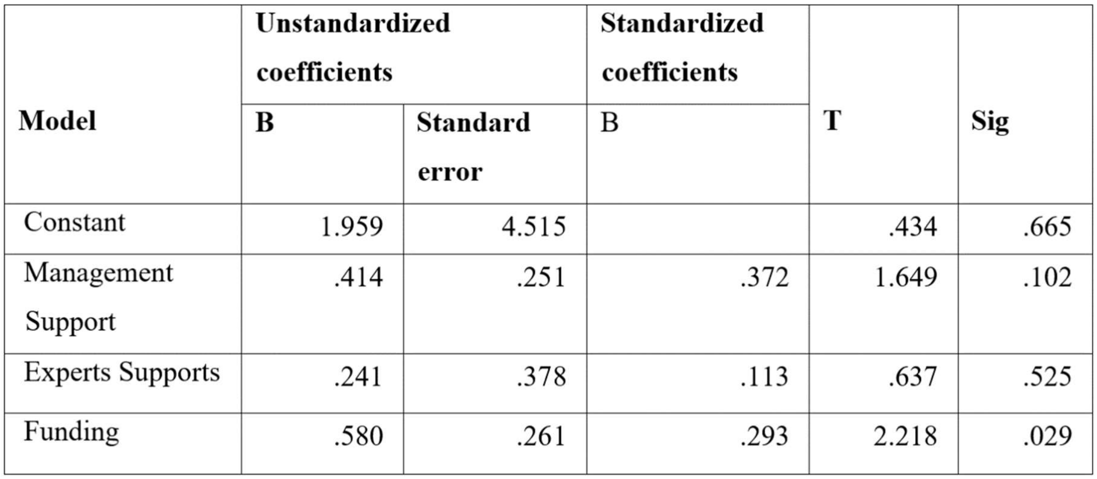
R= 0.557					**Adjusted R^2**= 0.281
R^2= 0.310					**Standard error**= 5.45102
Model	**SS**	**DF**	**MS**	**F**	**Sig**
Regression	1268.451	4	317.113	10.672	.000[b]
Residual	2822.796	95	29.714		
Total	4091.247	99			

Table 5: Joint Contributions of the Variables on ISRM

Table 5 reveals the joint contribution of management support, technical experts' supports, funding, and users' security awareness on risk assessment among the bank employees/customers. The R coefficient recorded 0.557, R2=0.310, when factor variables are combined, they explain 28.1% variance in risk assessment. 71.9% unexplained variance is as a result of variance outside the study. Therefore, there is a significant joint contribution of management support, experts' supports, funding, and users' security awareness on risk assessment among the banks; F (4, 95) = 10.672, P<0.01.

4.5 Relative Contribution of the Variables

Relative contribution of management support, experts' supports, funding, and users' security awareness on IS risk assessment is seen in the below table 6.



Model	Unstandardized coefficients		Standardized coefficients	T	Sig
	B	Standard error	B		
Constant	1.959	4.515		.434	.665
Management Support	.414	.251	.372	1.649	.102
Experts Supports	.241	.378	.113	.637	.525
Funding	.580	.261	.293	2.218	.029

Table 6: Relative Contribution of the Variables

Table 6 reveals that three out of the four factors (funding, management support, and users' security awareness) are significant predictors of risk assessment among banks. The most potent predictor of risk assessment is funding (β =0.293, t= 2.218, $p<0.05$), management support (β =0.372, t= 1.649, $p<0.05$) and users' security awareness (β= -0.234, t= -1.371, $p<0.05$) in contrast to experts supports (β=0.113, t= 0.637, $p>0.05$). This implies that, increase in funding will explain 29.3% increase in risk assessment, increase in management support will explain 37.2% increase in risk assessment and increase in user's security awareness will explain for 23.4% in risk assessment.

5 Analysis and Discussions

The main objective of this study was to explore the motivating factors influencing the implementation of information security risk management in the case of Nigerian Commercial Banks. This chapter presents the analysis of the results and their discussions.

The study used census to select 60 respondents from 10 commercial banks in Nigeria with emphasis on those within the southwestern states of Nigeria drawn from IT Security department, operation department, audit department, IT department, and risk management department. Forty responses were received; however, 15 questionnaires were rejected due to incompleteness. Thus, twenty-five responses were accepted for the study which represents a response rate of 62.5%.

The interviewees for the qualitative were chosen based on their responsibilities, job positions, and the number of years they have served in the banks. The interview was structured into five categories: First, the general questions, then cyber-risk measurement, influence of management support, influence of technical support, and influence of user's security awareness questions, and the conclusion. In the presentation of these empirical findings, bank one, two, three, four, etc was used as a synonym to represent the banks and respondents respectively. The pattern of the responses followed according to the structure of the interview guidelines. In some cases, the report from the respondent was quoted verbatim, as it relates to the banking policies and operations.

5.1 Qualitative Interview Transcript

This part is focused on the general questions to the respondents, their years of experience in the banking industry, their educational qualifications and positions held in the bank. The choice of respondents was based on experience both in theory and practice in the banking field, particularly with knowledge in information risk management together with years of experience in service. Although, it was not an easy task to have these respondents onboard for the interview, so, the first thing we did, was to send our topic and interview guide to the various bank respondents, and then asked them for a short interview in order to answer our research questions. However, our request was granted.

1. General Questions

Respondent 1 is the IT security manager for corporate clients in bank one. He is a master degree holder in Information technology. He has been working since 2016 in this present position putting in six years in service. Prior to that position, he was the head of the information security risk management section, where he was in charge of all risk management processes, identification of critical information assets, and evaluating them.

Respondent 2 is the Lead risk manager of the corporate financing in bank two. He is an MBA/Ph.D. holder in accounting and finance and has a working experience of seventeen years. Prior to his present position, he worked as an internal auditor in one of the investment companies for five years. He then moved to bank B as the cash officer specialist at different branches of the bank before settling in his present position.

Respondent 3 is the Bank internal controller in bank three. He is a master degree holder in economics, a professional chartered accountant (ACA), and a member of Chartered Institute of Bankers of Nigeria (ACIB). In his career path, he has been a risk management officer in bank three for five years but has worked in various branches of bank three in different positions. He possesses wealth of experience in banking operations.

Respondent 4 is the head of IT project manager in bank four. She is a master degree holder in Business Administration with specialization in project management. In her career path, she has been a risk management officer in bank four for three years, value and vendor manager for two years, in various branches of bank four. She possesses wealth of experience in banking operations and project governance at institutional levels.

The interview conducted under the general question had only four (4) respondents. Other six banks' respondents were not interviewed due to unavailability.

2. Cyber-Risk Measurement

Regarding the severity and measurement of information security risks (Cyber Risks) in the targeted banks, the interviewees were asked to measure and estimate the degree of risk factors regarding the cyber threats affecting the banks. The study used the risks measurement table shown below to document the degree of severity using either Low, Medium or High as shown by the table 7 below.

Cyber Threat	***Level of Severity/ Impact***	***Level of Severity/Impact***	***Level of Severity/Impact***	***Level of Severity/Impact***
Social Engineering (Phishing)	Proxies have demonstrated ability to destroy data or systems in this Bank (High)	Numerous campaigns or groups believed to target the Bank (Medium)	Bogus websites or fake online platforms, spam, or phishing emails, text messages, and social media posts to lure potential victims (Medium)	Phishing and other malicious actions through interactions and psychological manipulations that trick users to perform security mistakes or give away information (High)
Cyber Criminals	Cybercriminals have repeatedly and specifically targeted this Bank (High)	There is unauthorized user entry to the bank's systems and network undetected with the intention to steal financial and personal data, cyber money laundering, ATM, and credit card frauds (Medium)	High level of malware infections the Bank systems (Low)	Criminals have stolen large sums of money from the Bank. Cybercrime affecting the Bank is very sophisticated, relying on confidence scams or commodity malware (Medium)
Hacktivists	There is a frequent hacktivist target from multiple campaigns or groups (low)	Hacktivists have demonstrated ability to destroy data or systems in our Bank (Low)	Hacktivists frequently cause disruption to the Banks operations through their attacks (Low)	

Table 7: Cyber Risk Measurement in the Nigerian Banks

Bank 1: With respect to the statement regarding incidences of cyber criminals, the respondent from bank one stated that, the level of severity to cybercriminals repeatedly and specifically targeting this bank was high as indicated in table 7, while the statement that there is unauthorized user entry to the bank's systems and network undetected with the intention to steal financial and personal data scored a medium level of severity. The cyber money laundering, ATM, and credit card frauds scored a high level of severity, while the statement that there is a high level of malware infections in the bank's systems scored a lower level of severity. With regards to statement that criminals have stolen large sums of money from the bank, scored a medium level of severity.

The level of severity of Hacktivists incidences, in bank one shows that the frequency of hacktivist target from multiple campaigns or groups scored a low level of severity, while the statement that hacktivists have demonstrated ability to destroy data or systems in the bank scored a low level of severity. Finally, regarding the statement that Hacktivists frequently cause disruption to the bank's operations through their attacks scored a low level of severity.

Bank 2: With respect to statements regarding social engineering (Phishing) attacks, bank two stated that proxies ability to destroy data or systems in this bank presents a high risk; while numerous campaigns or groups believed to target the bank scored a medium risk; Bogus websites or fake online platforms, spam, or phishing emails, text messages, and social media posts to lure potential victims scored a medium risk; while phishing and other malicious actions through interactions and psychological manipulations that trick users to perform security mistakes or give away information scored a high risk.

With respect to statement regarding incidences of cyber criminals, bank two stated that the level of severity to cybercriminals repeatedly and specifically targeted this bank was medium; while the statement that there is unauthorised user entry to the bank's systems and network undetected with the intention to steal financial and personal data scored a high level of severity, the cyber money laundering, ATM, and credit card frauds scored a high level of severity; while the statement that there is a high level of malware infections the bank systems scored a medium level of severity. Regarding the statement that criminals have stolen large sums of money from the bank scored a low level of severity.

Regarding statements indicating the level of severity of Hacktivists incidences, bank two stated the frequency of frequent hacktivist target from multiple campaigns or groups scored a medium level of severity; while the statement that hacktivists have demonstrated ability to destroy data or systems in our bank scored a medium level of severity. Finally, regarding the statement that Hacktivists frequently cause disruption to the bank's operations through their attacks scored a low level of severity.

Bank 3: Regarding social engineering (Phishing) attacks, bank three stated that proxy's ability to destroy data or systems in this bank presents a low risk; while numerous campaigns or groups believed to target the bank scored a medium risk; Bogus websites or fake online platforms, spam, or phishing emails, text messages and social media posts to lure potential victims scored a high risk; while phishing and other malicious actions through interactions and psychological manipulations that trick users to perform security mistakes or give away information scored a high risk.

In respect to statement regarding incidences of cyber criminals, bank three stated that the level of severity to cybercriminals repeatedly and specifically that targeted this bank was medium; while the statement that there is unauthorised user entry to the bank's systems and network undetected with the intention to steal financial and personal data scored a medium level of severity. The cyber money laundering, ATM, and credit card frauds scored a high level of severity; while the statement that there is a high level of malware infections the bank systems scored a lower level of severity. Regarding the statement that criminals have stolen large sums of money from the bank scored a high level of severity.

Regarding statements indicating the level of severity of Hacktivists incidences, bank three stated that the frequency of frequent hacktivist target from multiple campaigns or groups scored a low level of severity; while the statement that hacktivists have demonstrated ability to destroy data or systems in our bank scored a medium level of severity. Finally, in regard to the statement that Hacktivists frequently cause disruption to the Banks operations through their attacks scored a low level of severity.

In respect to statements regarding social engineering (Phishing) attacks, bank three stated that proxies ability to destroy data or systems in this bank presents a low risk; while numerous campaigns or groups believed to target the bank scored a medium risk; Bogus websites or fake online platforms, spam, or phishing emails, text messages, and social media posts to lure potential victims scored a high risk; while phishing and other malicious actions through interactions and psychological manipulations that trick users to perform security mistakes or give away information scored a high risk.

Bank 4: With respect to statement regarding incidences of cyber criminals, bank four stated that the level of severity to cybercriminals repeatedly and specifically targeted this bank was low; while the statement that there is unauthorised user entry to the bank's systems and network undetected with the intention to steal financial and personal data scored a high level of severity, the cyber money laundering, ATM, and credit card frauds scored a high level of severity; while the statement that there is a high level of malware infections the bank systems scored a lower level of severity. Regarding the statement that criminals have stolen large sums of money from the bank scored a high level of severity.

Regarding statements indicating the level of severity of Hacktivists incidences, bank four stated the frequency of frequent hacktivist target from multiple campaigns or groups scored a medium level of severity; while the statement that hacktivists have demonstrated ability to destroy data or systems in our bank scored a low level of severity. Finally, in regard to the statement that Hacktivists frequently cause disruption to the Banks operations through their attacks scored a low level of severity.

Bank 5: In respect to statements regarding social engineering (Phishing) attacks, bank five stated that proxies ability to destroy data or systems in this bank presents a medium risk; while numerous campaigns or groups believed to target the bank scored a medium risk; Bogus websites or fake online platforms, spam, or phishing emails, text messages, and social media posts to lure potential victims scored a high risk; while phishing and other malicious actions through interactions and psychological manipulations that trick users to perform security mistakes or give away information scored a high risk.

In respect to statement regarding incidences of cyber criminals, bank five stated that the level of severity to cybercriminals repeatedly and specifically targeted this bank was high; while the statement that there is unauthorised user entry to the bank's systems and network undetected with the intention to steal financial and personal data scored a high level of severity, the cyber money laundering, ATM, and credit card frauds scored a high level of severity; while the statement that there is a high level of malware infections the bank systems scored a lower level of severity. Regarding the statement that cybercriminals have stolen large sums of money from the bank scored a high level of severity.

Regarding statements indicating the level of severity of Hacktivists incidences, bank five stated the frequency of frequent hacktivist target from multiple campaigns or groups scored a low level of severity; while the statement that hacktivists have demonstrated ability to destroy data or systems in the bank scored a medium level of severity. Finally, regarding the statement that Hacktivists frequently cause disruption to the banks operations through their attacks scored a low level of severity.

Bank 6**:** In respect to statements regarding social engineering (Phishing) attacks, bank six stated that proxies ability to destroy data or systems in this bank presents a medium risk; while numerous campaigns or groups believed to target the bank scored a medium risk; Bogus websites or fake online platforms, spam, or phishing emails, text messages and social media posts to lure potential victims scored a high risk; while phishing and other malicious actions through interactions and psychological manipulations that trick users to perform security mistakes or give away information scored a high risk.

In respect to statement regarding incidences of cyber criminals, bank six stated that the level of severity to cybercriminals repeatedly and specifically targeted this Bank was medium; while the statement that there is unauthorised user entry to the bank's systems and network undetected with the intention to steal financial and personal data scored a medium level of severity, the cyber money laundering, ATM, and credit card frauds scored a high level of severity; while the statement that there is a high level of malware infections the bank systems scored a lower level of severity. Regarding the statement that criminals have stolen large sums of money from the bank scored a high level of severity.

Regarding statements indicating the level of severity of Hacktivists incidences, bank six stated the frequency of frequent hacktivist target from multiple campaigns or groups scored a high level of severity; while the statement that hacktivists have demonstrated ability to destroy data or systems in our bank scored a medium level of severity. Finally, regarding the statement that Hacktivists frequently cause disruption to the banks operations through their attacks scored a low level of severity.

Bank 7**:** In respect to statements regarding social engineering (Phishing) attacks, bank seven stated that proxies ability to destroy data or systems in this bank presents a high risk; while numerous campaigns or groups believed to target the bank scored a low risk; Bogus websites or fake online platforms, spam, or phishing emails, text messages, and social media posts to lure potential victims scored a high risk; while phishing and other malicious actions through interactions and psychological manipulations that trick users to perform security mistakes or give away information scored a high risk.

In respect to statement regarding incidences of cyber criminals, bank seven stated that the level of severity to cybercriminals repeatedly and specifically targeted this bank was medium; while the statement that there is unauthorised user entry to the bank's systems and network undetected with the intention to steal financial and personal data scored a high level of severity, the cyber money laundering, ATM, and credit card frauds scored a high level of severity; while the statement that there is a high level of malware infections the bank systems scored a lower level of severity. Regarding the statement that criminals have stolen large sums of money from the bank scored a medium level of severity.

Regarding statements indicating the level of severity of Hacktivists incidences, bank seven stated the frequency of frequent hacktivist target from multiple campaigns or groups scored a low level of severity; while the statement that hacktivists have demonstrated ability to destroy data or systems in our bank scored a medium level of severity. Finally, regarding the statement that Hacktivists frequently cause disruption to the banks operations through their attacks scored a medium level of severity.

Bank 8: In respect to statements regarding social engineering (Phishing) attacks, bank eight stated that proxies ability to destroy data or systems in this bank presents a low risk; while numerous campaigns or groups believed to target the bank scored a medium risk; Bogus websites or fake online platforms, spam, or phishing emails, text messages, and social media posts to lure potential victims scored a high risk; while phishing and other malicious actions through interactions and psychological manipulations that trick users to perform security mistakes or give away information scored a high risk.

In respect to statement regarding incidences of cyber criminals, bank eight stated that the level of severity to cybercriminals repeatedly and specifically targeted this bank was medium; while the statement that there is unauthorised user entry to the bank's systems and network undetected with the intention to steal financial and personal data scored a high level of severity, the cyber money laundering, ATM, and credit card frauds scored a high level of severity; while the statement that there is a high level of malware infections the bank systems scored a lower level of severity. Regarding the statement that criminals have stolen large sums of money from the bank scored a medium level of severity.

Regarding statements indicating the level of severity of Hacktivists incidences, bank eight stated that the frequency of frequent hacktivist target from multiple campaigns or groups scored a high level of severity; while the statement that hacktivists have demonstrated ability to destroy data or systems in the bank scored a medium level of severity. Finally, regarding the statement that Hacktivists frequently cause disruption to the banks operations through their attacks scored a medium level of severity.

Bank 9**:** In respect to statements regarding social engineering (Phishing) attacks, bank nine stated that proxies ability to destroy data or systems in this bank presents a high risk; while numerous campaigns or groups believed to target the bank scored a medium risk; Bogus websites or fake online platforms, spam, or phishing emails, text messages, and social media posts to lure potential victims scored a high risk; while phishing and other malicious actions through interactions and psychological manipulations that trick users to perform security mistakes or give away information scored a high risk.

Furthermore, In respect to statement regarding incidences of cyber criminals, bank nine stated that the level of severity to cybercriminals repeatedly and specifically targeted this bank was medium; while the statement that there is unauthorised user entry to the bank's systems and network undetected with the intention to steal financial and personal data scored a high level of severity, the cyber money laundering, ATM, and credit card frauds scored a high level of severity; while the statement that there is a high level of malware infections the bank systems scored a lower level of severity. Regarding the statement that criminals have stolen large sums of money from the bank scored a high level of severity.

Regarding statements indicating the level of severity of Hacktivists incidences, bank nine stated the frequency of frequent hacktivist target from multiple campaigns or groups scored a high level of severity; while the statement that hacktivists have demonstrated ability to destroy data or systems in our bank scored a medium level of severity. Finally, regarding the statement that Hacktivists frequently cause disruption to the banks operations through their attacks scored a medium level of severity.

Bank 10: In respect to statements regarding social engineering (Phishing) attacks, bank ten stated that proxies ability to destroy data or systems in this bank presents a high risk; while numerous campaigns or groups believed to target the bank scored a medium risk; Bogus websites or fake online platforms, spam, or phishing emails, text messages, and social media posts to lure potential victims scored a high risk; while phishing and other malicious actions through interactions and psychological manipulations that trick users to perform security mistakes or give away information scored a high risk. In respect to statement regarding incidences of cyber criminals, bank ten stated that the level of severity to cybercriminals repeatedly and specifically targeted this bank was high; while the statement that there is unauthorised user entry to the bank's systems and network undetected with the intention to steal financial and personal data scored a high level of severity, the cyber money laundering, ATM, and credit card frauds scored a high level of severity; while the statement that there is a high level of malware infections the bank systems scored a medium level of severity. Regarding the statement that criminals have stolen large sums of money from the bank scored a high level of severity.

Regarding statements indicating the level of severity of Hacktivists incidences, bank ten stated the frequency of frequent hacktivist target from multiple campaigns or groups scored a high level of severity; while the statement that hacktivists have demonstrated ability to destroy data or systems in the bank scored a high level of severity. Finally, regarding the statement that Hacktivists frequently cause disruption to the banks operations through their attacks scored a high level of severity.

3. Influence of Management Support

Regarding the question whether the respondents believed that the quality of information security risks assessment in an organization is because of management support, 93% of the respondents agreed while 7% of the respondents disagreed. On those who agreed were requested to explain. The respondent from bank one stated the following: "*Employees can be integrated into the risk management process if there is a commitment from the management, in form of training and awareness, and exposing the criticality of the desired goal can be a motivating factor''.*

The respondent from bank two argued that: "*the level of seriousness attached to information security assessment by management through webinars and conferences can motivate employee's commitment".* This point is supported because it is a way of integrating the employees into the risk management culture in the organisation.

Another respondent from bank three stated "*that management support through provision of funds and resources to carry on information security risk management activities can spur interest among employees".*

The management has an audit and compliance team who regularly checks up on the banks and this really keeps us on our toes, according to respondents from bank two, three, six, seven and eight.

Furthermore, another respondent from bank four stated that banks has been mandated to establish compliance departments which has been in operation for years headed by executive director charge with ensuring full compliance to information.

When asked this question: *What are the challenges that are faced in users' security awareness in your organization? And how do you handle them?*

Respondent one simply stated that 80% of the employees/customers are ignorant and naive about IT security awareness. This confirmed the notion that humans are the weakest link in security chain. It went further to suggest that every employee and customers should be educated and create awareness for their IT security training.

The responses were also asked to choose the management support actions that aids IS risk assessment process in their organization. The study results indicate that 85% of respondents indicated that their bank offers support in the forms of skill; 93% indicated that monetary support is offered; 62% of respondents stated that there is direct participation in organization's risk management while 25% stated that they are involved in the budget approval. Furthermore, 16% stated that they are involved in the IS policy formulation, 12% stated that there exists team appointment in their bank while 45% stated that they are involved in the supervision and monitoring in the evaluation of IS protocols. These findings are as shown in the figure 8 below:

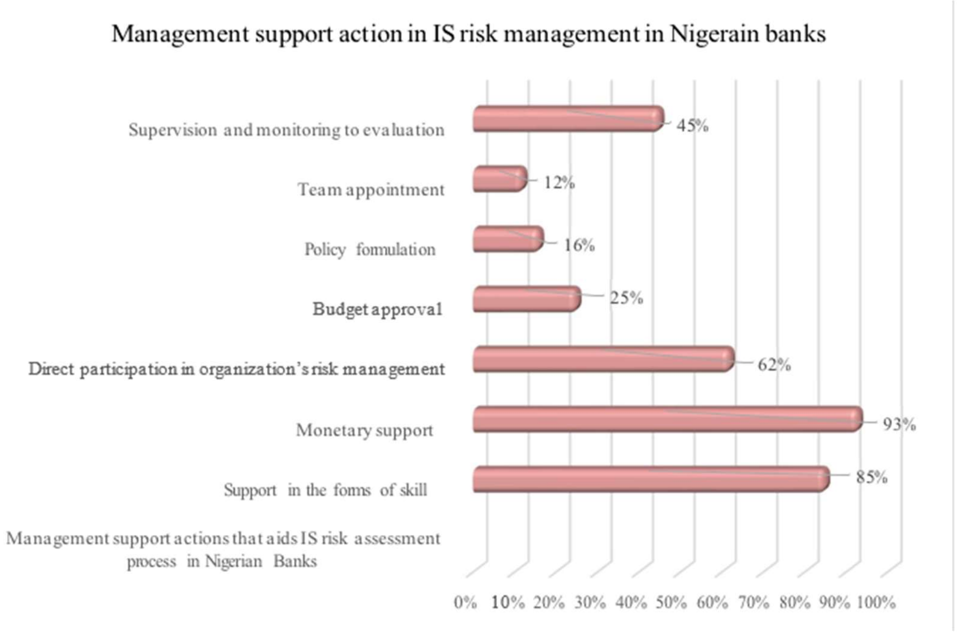


Figure 8: Management support actions that aids IS risk management in Nigerian Banks

- ***Relationship between management support and Information security risks management.***

The study sought to find out the extent of agreement with reference to statements regarding the influence of management support on information security risks assessment. From the findings, respondents agreed that; the firm has invested in high level innovation and technology to processes for risk assessment; the organization has integrated risk management into decision-making process will create efficiency in procedure and control in a common risk management; risk management assessment protects the entire management structure and measure the pattern of performance in relation to risk management; management support improves and support decision making in IS risk management; the management offers support in developing training programs, supporting quality management, formulating objectives and strategies for IS risk assessment; the level of capability in managing risk project administration in the organization has a connection with the IS risk assessment; top management commitment to the process of formulating strategic decisions is the key to successful risk assessment and performance efficiency; effective IS risk management implementation and objective accomplishment; compensated by top management as a reward for the success and that management's responsibility is to determine the types of countermeasures of the banks to minimize the information security risks within the organization as shown by means of 4.03, 3.83, 3.82, 3.68, 4.38, 4.04, 5.55 and 3.08 respectively.

Respondents were asked, why they think information assets need to be identified within the bank before classification?

A respondent from bank one stated that it will enable the bank to understand the value and worth of the assets in order to know the level of security needed to protect such information asset.

A respondent from bank two states that, Information asset is very crucial in today's modern banking. It helps banks to identify, classify and store information before its use. Information security risk management is a priority for decision making.

Furthermore, a question concerning the information security policies guiding the operation of their respective bank was asked, and a vivid answer was given, that the employees are under agreement not to disclose customers information or details. The same answer was also given by all the ten respondents.

Statement	***SA*** ***5***	***A*** ***4***	***N*** ***3***	***D*** ***2***	***S D*** ***1***	**Mean**	**Std** **Dev**
The banking industry has invested in high-level innovation and technology processes for risk assessment	24.9	1.9	16.1	1.9	0.6	4.03	1.55
Integrating risk management into decision-making process will create efficiency in procedure and control in a common risk management	12.7	62	21.5	3.5	0.3	3.83	1.03
IS risk management assessment protecting the entire management structure and measures the pattern of performance in relation to risk management.	52.90	17	25.8	0.3	3.9	3.82	1.09
Management support improves and support decision- making in IS risk management.	14.6	46.7	31.1	7	0.6	3.68	0.86
The management offers support in developing training programs, supporting quality management, and formulating objectives and strategies for IS risk assessment.	45.5	47.4	6.1	1.8	2.1	4.38	4.26
The level of capability in managing risk project administration in the organization has a connection with the IS risk assessment.	27.8	52.1	17.3	2.2	0.6	4.04	3.24
Top management commitment to the process of formulating strategic decisions is the key to successful risk assessment and performance efficiency.	79.6	58.5	0.3	0.1	0.2	5.55	5.65
Effective IS risk management implementation and objective accomplishment can be compensated by top management as a reward for the success	13.6	62.4	0.2	0.5	0.3	3.08	4.0

Table 8: Relationship between management support and Information security risk management.

Also, about the question about "*If information security risk management is aligned to your banks' business objectives?"* was asked.

All respondent bank stated that information security risk management is a major business objective to the banks and that central bank of Nigeria (CBN) has mandated all commercial banks to establish security risk management and business continuity departments to monitor the compliance of this policy. Employees have intensively been instructed that information about customers details/account should not be disclosure to anybody. Even if the instructions are coming from federal government agencies such as (ICPC) Independent Corrupt Practices and Other Related Offences Commission, nor the Economic and Financial Crimes Commission (EFCC) which is a Nigerian law enforcement agency that investigates financial crimes such as advance fee fraud (419 fraud) and money.

4. Influence of Technical Experts' Support

The first interview question under this section was: *What has the technical experts contributed so far to improving the information security posture of your bank?*

Bank one stated that the technical expert has been able to establish IT security awareness through e-learning across the entire bank, to motivate employees. Other respondents from bank two, three, four, five, eight and ten categorically stated that: "*Before now we hear so much complains about customers losing their money due to a mobile app creation they know nothing about, as a result of this the technical team devised a means that enables the mobile app to be only activated in the bank*". This has helped to reduce the rate of cyber fraud and manipulations of customers account and their BVN- Bank verification number.

Regarding the IS technical support experts that aids IS risk management in the Nigerian Banks, respondents were asked to state the ones that are utilized by their organizations. From the findings, 92% of the respondents indicated that their organization has network, system, application and database administrators, 98% of the respondents indicated that their banks hires computer specialists, 88% of the respondents indicated that their bank has security analysts while 69% indicated that their bank hires security consultants as shown in figure 9 below.

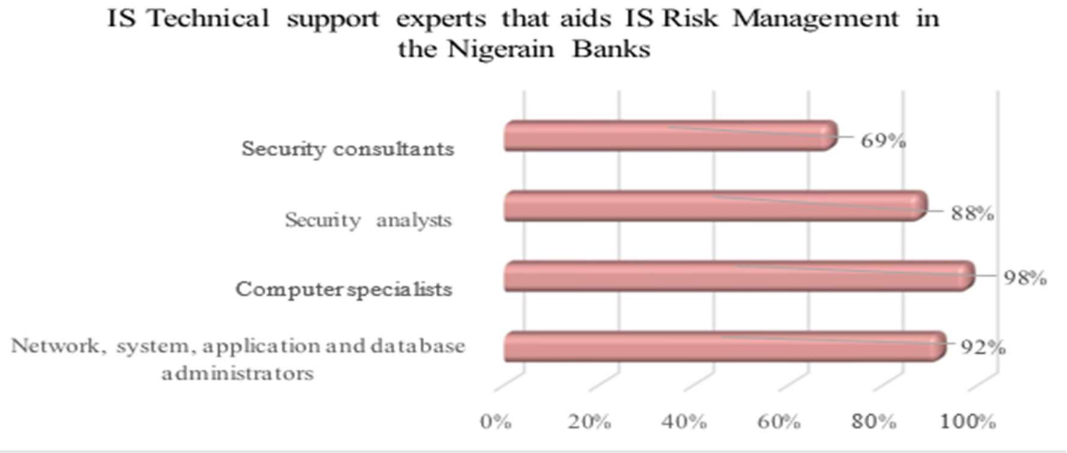


Figure 9: IS technical support & IS risk management

Figure 9 shows a bar chart showing the extent of agreement with statements regarding the influence of technical experts support on information security risks assessment that was established.

From the findings, respondents agreed that the firm has invested in competent information system experts to create seamless IS risk management assessment; IT security practitioners are responsible for proper implementation of security requirements in their IT systems; the IT security practitioners in my organization supports and apply use the risk management process to identify and assess potential IS risks and that the technical support team manages changes that occur in the existing IT system environment (e.g., expansion in network connectivity, changes to the existing infrastructure and organizational policies, introduction of new technologies to enhance IS risk management process as shown by means of 5.9, 6.35, 6.0 and 6.79 respectively as shown in the table 9 below.

	SA	***A***	***N***	***D***	***SD***		***Std***
Statement	***5***	***4***	***3***	***2***	***1***	***Mean***	***Dev***
The firm has invested in competent information system experts to create seamless IS risk management assessment	69.20	58.6	14.7	4.5	0.45	5.9	1.04
IT security practitioners are responsible for proper implementation of security requirements in their IT systems	77.8	60.6	14.25	5.7	0.3	6.35	0.61
The IT security practitioners in my organization supports and apply use the risk management process to identify and assess potential IS risks and that the technical support team manages changes that occur in the existing IT system environment (e.g., expansion in network connectivity, changes to the existing infrastructure	79.6	51.6	12.5	6.4	0.25	6.0	0.92
Organizational policies, introduction of new technologies to enhance IS risk management process	69.75	8.5	8.5	2.5	88.3	6.79	0.69

Table 9: IS technical expert support

5. Influence of Users' Security Awareness

Respondents were asked to enumerate the users' security awareness strategies that their organization has put in place to in order to create user's information security awareness. From the findings majority of the respondents stated the following as some of the security awareness strategies used in their banks; awareness training by educating staff on the cyber threats faced, raising awareness of the sensitivity of data on systems, providing information on how to avoid Phishing emails and other scam tactics, building a culture of enhanced security compliance, showing live attacks happening on their networks to further hammer home the message, staging simulated social engineering attacks (penetration tests) to assess whether the number of employees falling for them is dropping, demonstrating for employees how poor security practices can lead to harm to the company and clearly expressing the level of risk their omissions brings, offering refresher sessions as well as through mediums like blogs, posters and newsletters,

The respondents were also asked to indicate the areas in which their organization has embraced user's security awareness in order to enhance information security risks assessment. From the findings, majority of the respondents identified personal data of banking customers, Bank's records, user data such as login credentials and credit card numbers, computer networks, bank's digital infrastructure as the areas in which their organization has embraced user's security awareness in order to enhance information security risks assessment.

The respondents were also asked to mention the challenges that are faced in users' security awareness in their organization and how they are handled. From the findings, respondents provided the following challenges and remedies as shown in table 10 below:

Challenges	***How it is handled***	***Percentage of the respondents***
Change Resistance challenge	Requiring attendance at times or places, make the course content as convenient as possible, weaving it into employees' daily routines rather than making it a burdensome addition. Establish a short, consistent content length so employees never dread being stuck in a session when they're eager to get back to their work.	75%
Training awareness issues	Select a program that offers fresh, relevant, and stimulating content. Enlist well-established training techniques such as interactivity, clarity, relevance, and a judicious use of video to be both informative and engaging	62%
Inadequate learning resources	Introduce micro learning, which strategically breaks content into frequent, engaging, lessons of three minutes or less. Refreshing a learner's memory soon after first being exposed to new material is the key to retention	87%
Lack of onboarding process for employees	Designing a program to build a strong organizational culture and helping in ensuring all employees participate, learn, remember and routinely apply the learned material.	76%

Table 10: Challenges facing Users' Security Awareness in Nigerian Banks and how they are handled.

The extent of agreement with statements regarding relationship between product diversification strategies and market share was established as shown in table 11.

The study sought to find out the extent to which respondents agree with each of the statements regarding the relationship between Users' security awareness on information security risks assessment. From the findings, respondents agreed that the use of the IT systems and data according to an organization's policies, guidelines, and rules of behaviour is critical to mitigating risk and protecting the organization's IT resources. To minimize risk to the IT systems, it is essential that system and application users be provided with security awareness training. The IT security trainers or security professionals must understand the risk management process so that they can develop appropriate training materials and incorporate risk assessment into training programs to educate the end users, and that security awareness training helps the organization save significant financial resources by lowering the chance of a cyber-breach through human error as shown by means of 7.54, 7.36, 7.77 and 4.83 respectively.

Statement	***SA*** ***5***	***A*** ***4***	***N*** ***3***	***D*** ***2***	***SD*** ***1***	**Mean**
Use of the IT systems and data according to an organization's policies, guidelines, and rules of behaviour is critical to mitigating risk and protecting the organization's IT resources.	96.3	91.6	0.6	0	0	7.54
To minimize risk to the IT systems, it is essential that system and application users be provided with security awareness training.	91.8	86	5.8	0.3	0.1	7.36
The IT security trainers or security/subject matter professionals must understand the risk management process so that they can develop appropriate training materials and incorporate risk assessment into training programs to educate the end users	95.6	92	0.9	5.3	0.4	7.77
Security awareness training helps the organization save significant financial resources by lowering the chance of a cyberbreach through human error.	37	59	20	1.5	3.2	4.83

Table 11: Relationship between Security Awareness and ISRM

Table 11 explains the extent to which respondents agreed with each of the statements regarding the relationship between Users' Security Awareness and information security risks assessment. The following were the last segment of interview that was carried out before the session was closed.

What are the challenges that are faced in users' security awareness in your organization? And how do you handle them?

Respondents from bank two, five, eight, and nine stated that human factor is the biggest challenge because that where the vulnerabilities are much. Also lack of awareness and being naive when it comes to security posture.

What are the most frequent cyber risks that your bank faces?

Respondents stated that fraudulent calls are always flooding the bank hotlines upon creation of new accounts. Email phishing, appear phishing, and vishing attacks.

How can these risks be controlled or mitigated?

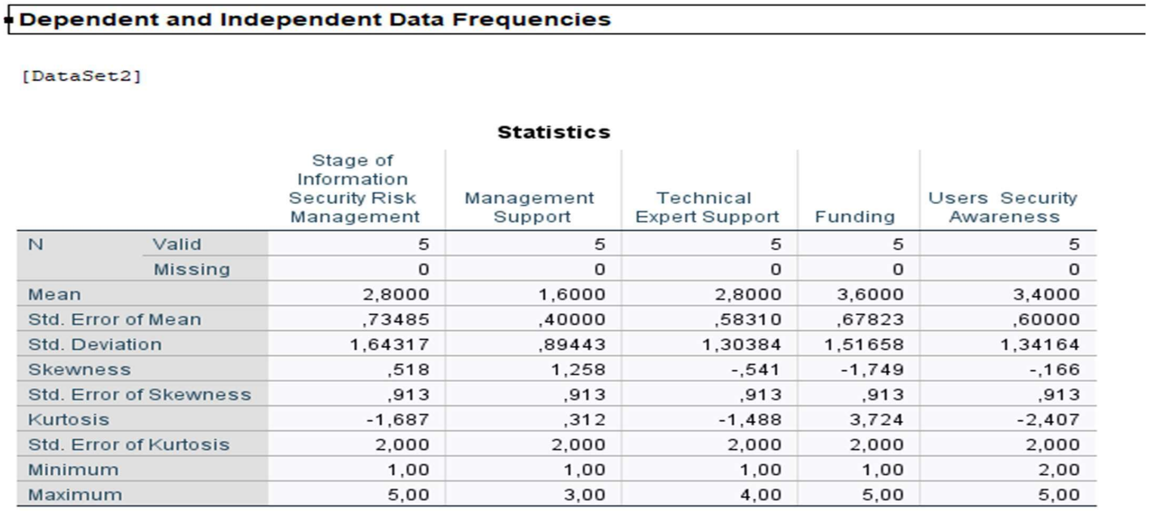
Respondents stated that it is through constant e-learning, training and sending simulation phishing mail to staff to see if they can identify a phishing mail.

The interview was concluded with this last question: We wanted to know the areas there could be changes in the banking industry to enhance the ISRM. *What change do you hope can take place in the banking industry to improve ISRM implementation?*

Respondents from various banks two, four, six, eight and nine shared almost the same idea, and for the sake of brevity, the findings are summarised as thus:
The banks have started implementing changes already though in the aspect of the mobile app and this would go a long way if upon registering a new customer, the ATM card and details of the customer are needed, most banks have this and I think it will go a long way to limit fraudulent transaction via mobile app.

5.2 Descriptive Statistics Analysis of the Variables

Under this section, we analyse the computation and calculation of the statistical values of the dependent and independent variables, taking into consideration the statistical values of the standard deviation, correlation, mean, as well as the minimum and maximum values of the overall variables. The descriptive statistical analysis involves entering the data, do a frequency count and calculation of the central tendency, and measures of variability. The mean signifies the average height, and the standard deviation tells us about how large the height is spread out within the average. The independent variables reoccur continuously on a Likert-scale of five (levels), while the dependent variable remain constant. From SPSS calculation, we derived the descriptive Statistics correlation frequencies:



Dependent and Independent Data Frequencies

[DataSet2]

Statistics

		Stage of Information Security Risk Management	Management Support	Technical Expert Support	Funding	Users Security Awareness
N	Valid	5	5	5	5	5
	Missing	0	0	0	0	0
Mean		2,8000	1,6000	2,8000	3,6000	3,4000
Std. Error of Mean		,73485	,40000	,58310	,67823	,60000
Std. Deviation		1,64317	,89443	1,30384	1,51658	1,34164
Skewness		,518	1,258	-,541	-1,749	-,166
Std. Error of Skewness		,913	,913	,913	,913	,913
Kurtosis		-1,687	,312	-1,488	3,724	-2,407
Std. Error of Kurtosis		2,000	2,000	2,000	2,000	2,000
Minimum		1,00	1,00	1,00	1,00	2,00
Maximum		5,00	3,00	4,00	5,00	5,00

Table 12: Dependent and Independent Data Frequencies.

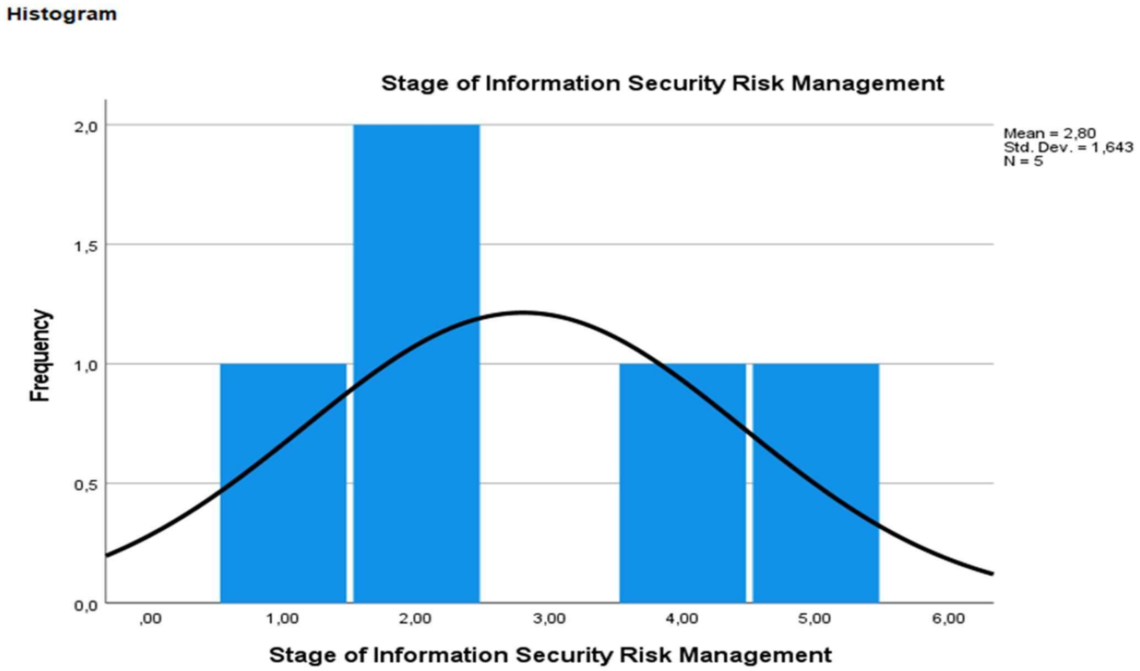


Figure 10: Stage of information security risk management showing the mean and standard deviation and dimension.

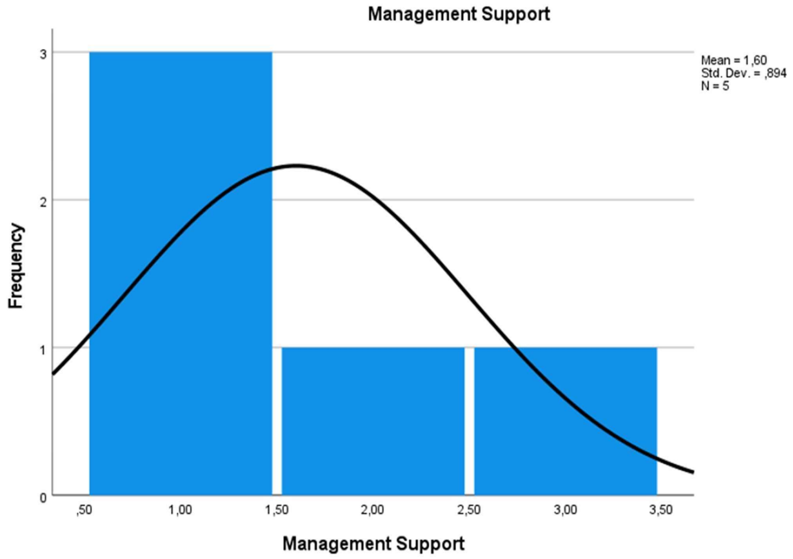


Figure 11: Influence of Management Support on ISRM showing the mean and standard deviation and dimension.

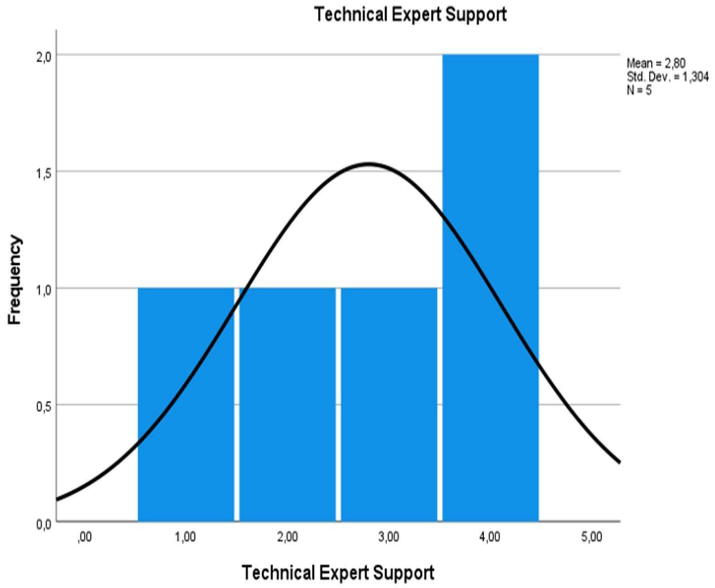


Figure 12: Influence of Technical Expert Support on ISRM showing the mean and standard deviation and dimension.

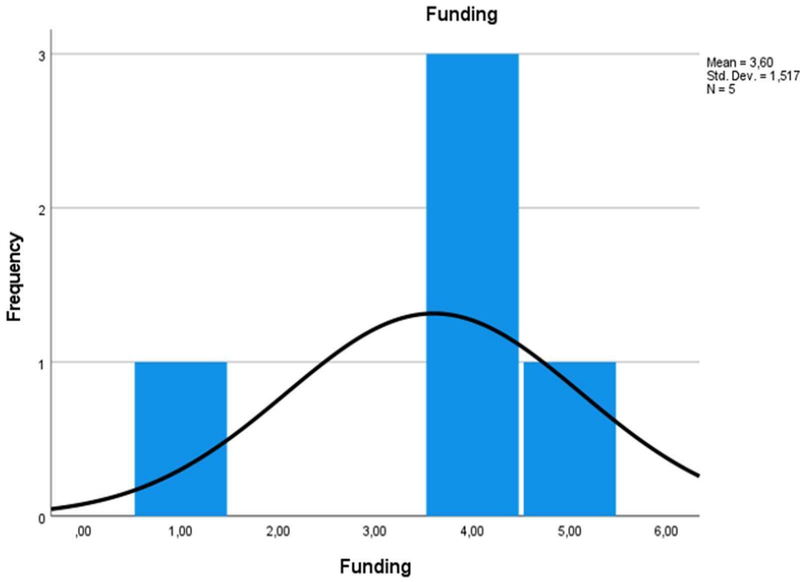


Figure 13: Influence of funding on information security risk management showing the mean and standard deviation and dimension.

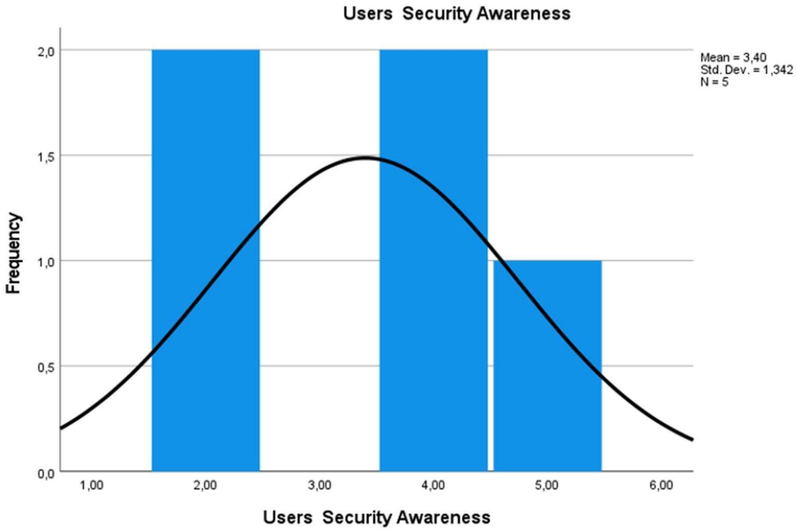
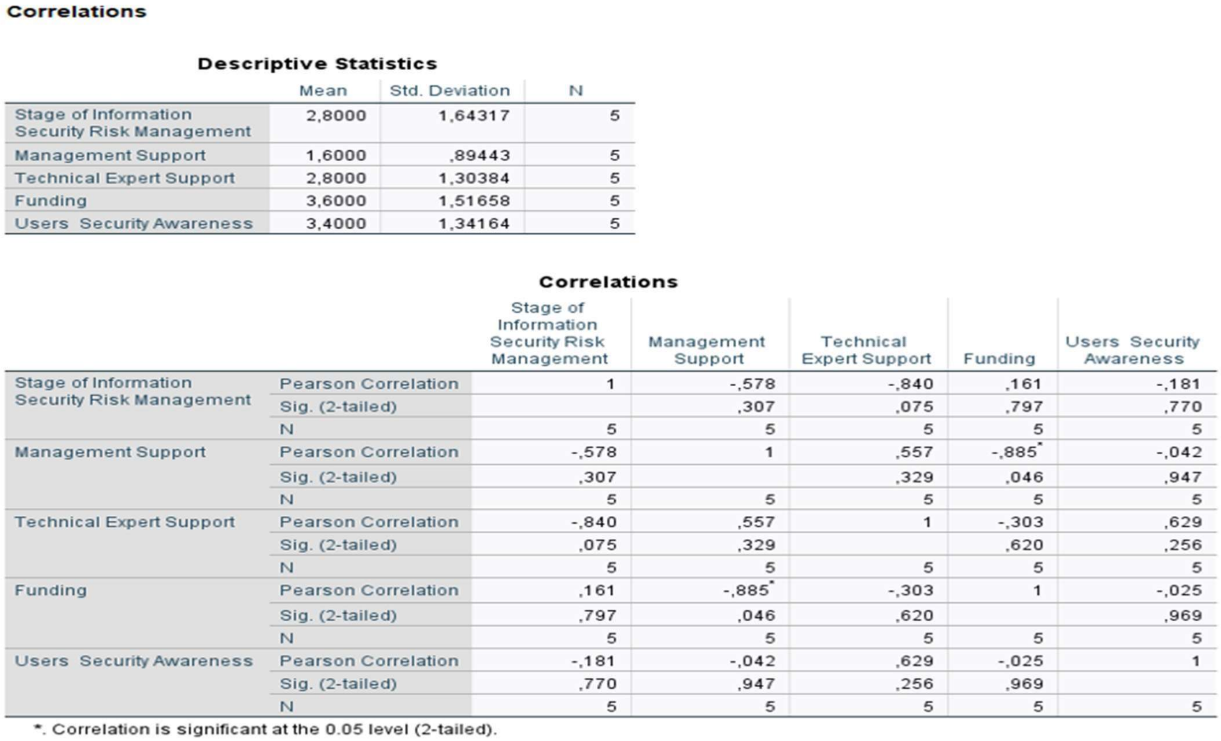


Figure 14: Influence of User Security Awareness on ISRM showing the mean and standard deviation and dimension.

5.3 Multiple Collinearity

The descriptive statistic shows that the minimum value of mean of independent variable is 1.6 and the maximum is 3.6. The predictors (constant) variable mean is 2.7, while the lowest standard deviation value of the independent variables is 0.89, while the maximum value is 1.5. The Pearson correlation of the independent variables are significant because the threshold of the value is 1. One can justify that the independent variables have no multicollinearity issues among the variables under research.

However, the Pearson correlation reveals that the stage of information security risk management in Nigerian banking sector are not fully in place. Throughout the correction analysis, the relationship between the dependent variable (SISRM) and the predictors were negatively impacted. This justifies the use of multiple logistic regression model to determine the relative importance of each of the variables with respect to factors influencing information security risks management in Nigerian commercial banks. The reason being that the dichotomous dependent variable (SISRM) negates the normality assumption that all things being equal, the stage of information security risk management supposed to be in place.



Correlations

Descriptive Statistics

	Mean	Std. Deviation	N
Stage of Information Security Risk Management	2,8000	1,64317	5
Management Support	1,6000	,89443	5
Technical Expert Support	2,8000	1,30384	5
Funding	3,6000	1,51658	5
Users Security Awareness	3,4000	1,34164	5

Correlations

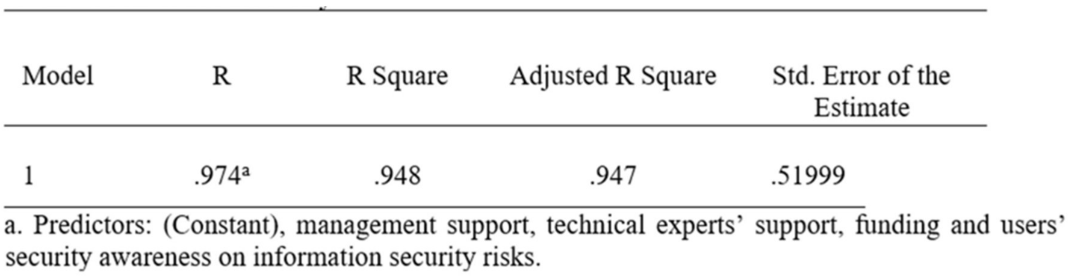
		Stage of Information Security Risk Management	Management Support	Technical Expert Support	Funding	Users Security Awareness
Stage of Information Security Risk Management	Pearson Correlation	1	-,578	-,840	,161	-,181
	Sig. (2-tailed)		,307	,075	,797	,770
	N	5	5	5	5	5
Management Support	Pearson Correlation	-,578	1	,557	-,885*	-,042
	Sig. (2-tailed)	,307		,329	,046	,947
	N	5	5	5	5	5
Technical Expert Support	Pearson Correlation	-,840	,557	1	-,303	,629
	Sig. (2-tailed)	,075	,329		,620	,256
	N	5	5	5	5	5
Funding	Pearson Correlation	,161	-,885*	-,303	1	-,025
	Sig. (2-tailed)	,797	,046	,620		,969
	N	5	5	5	5	5
Users Security Awareness	Pearson Correlation	-,181	-,042	,629	-,025	1
	Sig. (2-tailed)	,770	,947	,256	,969	
	N	5	5	5	5	5

*. Correlation is significant at the 0.05 level (2-tailed).

Table 13: Descriptive statistics and the correlation.

5.4 Regression Analysis

Having considered each factor singly a multi-regression was generated to establish the collective influence of management support, technical experts' support, funding and users' security awareness on information security risks on information security risks assessment. The multiple regression analysis also provided the relative importance of each of the variable with respect to the factors influencing the implementation of information security risk management in the case of Nigerian Commercial Banks. This section presents a discussion of the results of inferential statistics.



Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.974^a	.948	.947	.51999

a. Predictors: (Constant), management support, technical experts' support, funding and users' security awareness on information security risks.

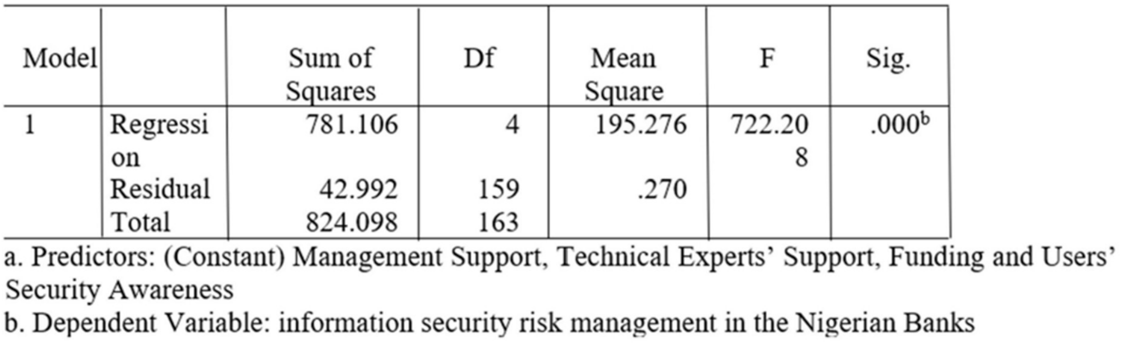
Table 14: Model Summary- Regression analysis

5.5 Survey Data, 2022

a. Predictors: (Constant), management support, technical experts' support, funding and users' security awareness on information security risks.

b. Dependent Variable: information security risk management

Coefficient of determination explains the extent to which changes in the dependent variable can be explained by the change in the independent variables or the percentage of variation in the dependent variable (Factors influencing the implementation of information security risk management) that is explained by all the four independent variables (management support, technical experts' support, funding and users' security awareness on information security risks). The four independent variables that were studied, explain 94.8 percent of variance in influence of strategic responses on information security risk management in Nigerian commercial Banks by the R^2. This therefore means that other factors not studied in this research contribute 5.2 percent of variance in the dependent variable. Therefore, further research should be conducted to evaluate the other factors that influence of information security risk management in the Nigerian Banks.



Model		Sum of Squares	Df	Mean Square	F	Sig.
1	Regression	781.106	4	195.276	722.208	.000[b]
	Residual	42.992	159	.270		
	Total	824.098	163			

a. Predictors: (Constant) Management Support, Technical Experts' Support, Funding and Users' Security Awareness

b. Dependent Variable: information security risk management in the Nigerian Banks

Table 15: Anova- Analysis of variance

5.6 Source: Research Data, 2022

The F critical at five percent level of significance was 2.27. Since F calculated is greater than the F critical (value =722.208), this shows that the overall model was significant. The significance is less than 0.05, thus indicating that the predictor variables, explain the variation in the dependent variable which is the factors influencing the implementation of information security risk management in the case of Nigerian Commercial Banks. If the significance value of F was larger than 0.05 then the independent variables would not explain the variation in the dependent variable.

5.7 Multiple Regression Analysis

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		b.	Std. Error	Beta		
1	(Constant)	.446	.172		2.598	.010
	Users' Security Awareness	.083	.018	.248	4.568	.000
	Funding	.181	.019	.467	9.402	.000
	Technical Experts' Support	.023	.012	.082	1.900	.009
	Management Support	.088	.020	.216	4.489	.000

Table 16: Multiple Regression Analysis

a. Predictors: (Constant), management support, technical experts' support, funding and users' security awareness.

b. Dependent Variable: information security risk management in the Nigerian Banks

A multiple logistic regression model was applied to determine the relative importance of each of the variables with respect to factors influencing information security risks management in Nigerian commercial banks.

Y = ß0+ ß1, MS + ß2, TES + ß3, F + ß4, UAT + 0e

Therefore, Y = .446+ .088MS + .023TES + .181F + .083UAT + 0e

Where:

Y = represents the Stage of Information Security Risk (SISRM) Management (Dependent variable) ß0 = represents a constant value, or value of SISRM when all dependent variables are 0.

ß1, ß2, ß3, and ß4 = represent the regression coefficients for the relevant variables

MS = Management Support (Independent Variable)

TES = Technical Experts' Support (Independent Variable)

F= Funding (Independent Variable)

UAT = Users' Security Awareness (Independent Variable)

e = error term. This may not include the effect of variables in the model for the "term" (t)

The categorical dependent variable, STAGE of ISRM IMPLEMENTATION, reflects a static variable. Value of 1 or 0 denotes the following:

ISRM stage of implementation =1, if ISRM is in place.

ISRM stage of implementation =0, if ISRM is not fully in place.

The other independent variables can be regarded as a continuous variable which can be measured by Likert scale between 1 to 5, where 1 = strongly disagree and 5 = strongly agree.

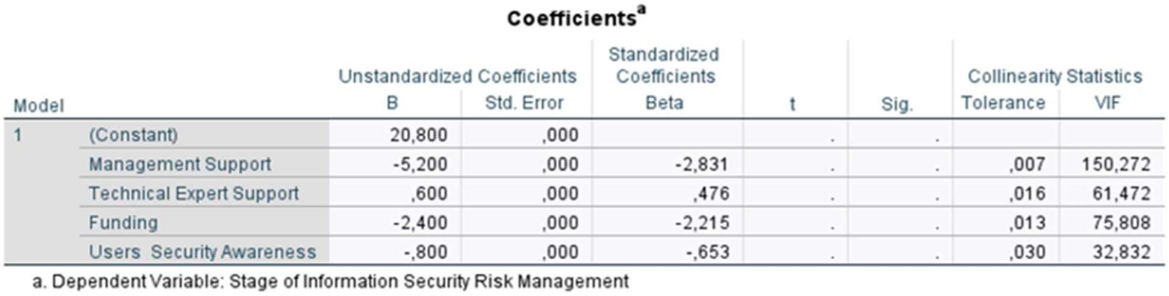
According to the equation, taking all factors (management support, technical experts' support, funding and users' security awareness) constant at zero, factors influencing the implementation of information security risk management in the case of Nigerian Commercial Banks showed .446 coefficient value. The data findings also show that a unit increase in Management Support variable will lead to a .088 coefficient increase in the level of information security risk management in the Nigerian Banks; a unit increase in technical experts' support will lead to .023 increase in the level of information security risk management in the Nigerian Banks; a unit increase in funding will lead to a 0.181 increase in the level of information security risk management in the Nigerian Banks and a unit increase in users' security awareness will lead to a .083 increase in the level of information security risk management in the Nigerian Banks.

Therefore, from these results, funding contributes most to level of information security risk management in the

Nigerian Banks at 0.181 followed by management support at 0.088, followed by users' security awareness at

0.083 and the least contributor is technical experts' support scoring the lowest at 0.023.

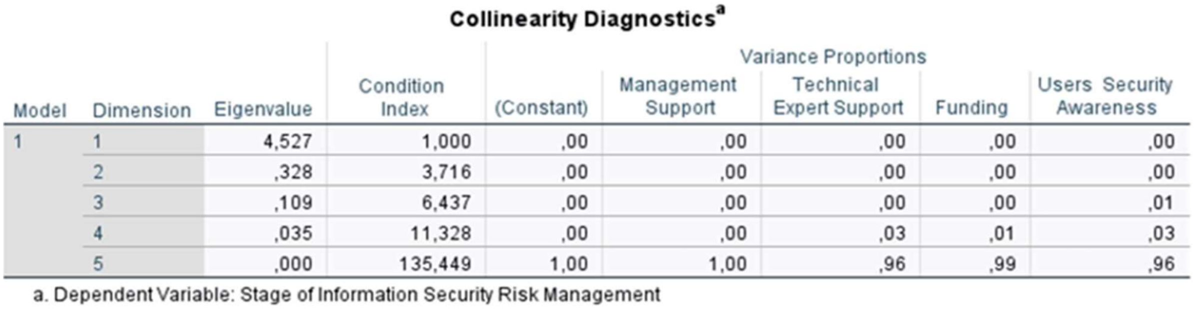
5.8 Logistic Regression Summarization



Coefficients^a

		Unstandardized Coefficients		Standardized Coefficients			Collinearity Statistics	
Model		B	Std. Error	Beta	t	Sig.	Tolerance	VIF
1	(Constant)	20,800	,000		.	.		
	Management Support	-5,200	,000	-2,831	.	.	,007	150,272
	Technical Expert Support	,600	,000	,476	.	.	,016	61,472
	Funding	-2,400	,000	-2,215	.	.	,013	75,808
	Users Security Awareness	-,800	,000	-,653	.	.	,030	32,832

a. Dependent Variable: Stage of Information Security Risk Management



Collinearity Diagnostics^a

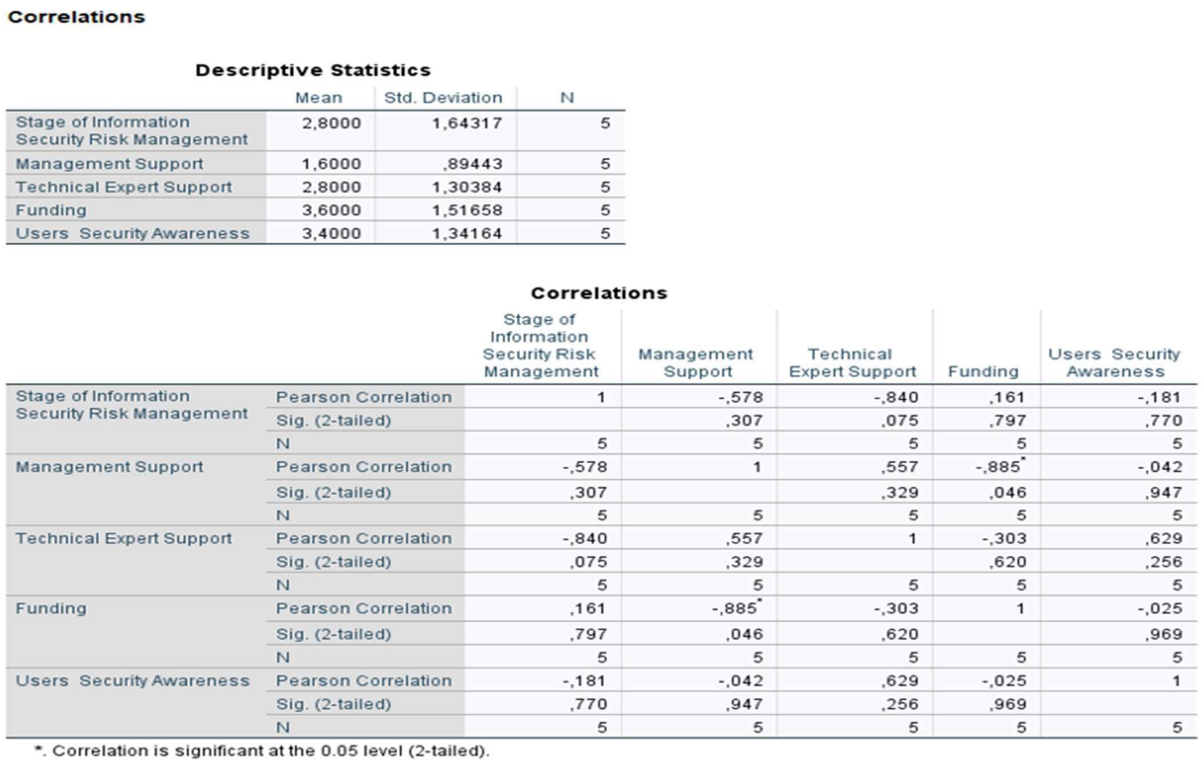
				Variance Proportions				
Model	Dimension	Eigenvalue	Condition Index	(Constant)	Management Support	Technical Expert Support	Funding	Users Security Awareness
1	1	4,527	1,000	,00	,00	,00	,00	,00
	2	,328	3,716	,00	,00	,00	,00	,00
	3	,109	6,437	,00	,00	,00	,00	,01
	4	,035	11,328	,00	,00	,03	,01	,03
	5	,000	135,449	1,00	1,00	,96	,99	,96

a. Dependent Variable: Stage of Information Security Risk Management

Table 17: Logistic Regression Summarization

The above tables reflect the result of the logistic regression coefficient and collinearity diagnostics analysis performed to measure the influence of the stage of information security risk management (dependent variable) in Nigerian commercial banks using the independent variables: (MS = Management Support, TES = Technical Experts' Support, F= Funding, UAT = Users' Security Awareness).

The logistic regression model present and display the tests of coefficient, collinearity statistics, tolerance and VIF of the data analysis. In SPSS software, the Pearson correlation was deployed to derive the standardized and unstandardized coefficients with beta value.



Correlations

Descriptive Statistics

	Mean	Std. Deviation	N
Stage of Information Security Risk Management	2,8000	1,64317	5
Management Support	1,6000	,89443	5
Technical Expert Support	2,8000	1,30384	5
Funding	3,6000	1,51658	5
Users Security Awareness	3,4000	1,34164	5

Correlations

		Stage of Information Security Risk Management	Management Support	Technical Expert Support	Funding	Users Security Awareness
Stage of Information Security Risk Management	Pearson Correlation	1	-,578	-,840	,161	-,181
	Sig. (2-tailed)		,307	,075	,797	,770
	N	5	5	5	5	5
Management Support	Pearson Correlation	-,578	1	,557	-,885*	-,042
	Sig. (2-tailed)	,307		,329	,046	,947
	N	5	5	5	5	5
Technical Expert Support	Pearson Correlation	-,840	,557	1	-,303	,629
	Sig. (2-tailed)	,075	,329		,620	,256
	N	5	5	5	5	5
Funding	Pearson Correlation	,161	-,885*	-,303	1	-,025
	Sig. (2-tailed)	,797	,046	,620		,969
	N	5	5	5	5	5
Users Security Awareness	Pearson Correlation	-,181	-,042	,629	-,025	1
	Sig. (2-tailed)	,770	,947	,256	,969	
	N	5	5	5	5	5

*. Correlation is significant at the 0.05 level (2-tailed).

Table 18: Correlation featuring Descriptive Statistics.

From the table, it is clearly seen that there is no variable that is highly correlated with one another. The correlation values are below the threshold value of 0.9, meaning that there is no multicollinearity issues or problem associated with the variables under study.

6 Summary, Conclusion, and Recommendation

6.1 Summary

Considering the growing public outrage about cyber-attacks in Nigeria's banking industry prompted this investigation. There were 1,612 complaints from users of financial services about banking fraud and aggressive charges between July and December 2018; 99.38 percent of them were against commercial banks (Nelson, 2019). This reveals the banking industry's lack of information security management. This indicates that the primary goal of Information Security (IS) is to protect the business from threats and ensure daily operational success by ensuring confidentiality, integrity, availability, and non- repudiation (Wangen and Snekkenes, 2013). Therefore, this study investigated Factors Influencing the Implementation of Information Security Risk Management. A case study of Nigerian Commercial Banks.

This research study has investigated the factors influencing the implementation of information risk management in Nigerian commercial banks, using the independent variables- Management Support, Technical Experts' Support, Funding, and Users' Security Awareness, that were formulated. From the research questions. It is one of the very few research studies carried out in this area of research. The results drawn from our statistical analysis revealed that there is a correlation between all the independent variables and the dependent variable (stage of information security risk management). The banks that have good management support, well qualified IT experts, and good IT security training are more likely to strengthen the ISRM implementation faster and efficiently.

The ultimate contribution we found out is that top management support, the influence of the regulatory institution (CBN), management audit controlling system and training awareness of the employees, has most importantly influenced the implementation of information security risk management in Nigerian commercial banking industry. These findings were supported by Dabari, & Saidin, (2015), in a research study carried out on determinants factors influencing the implementation of enterprise risk management in the Nigerian banking sector. On the other hands, it is not all the banks that the stage of ISRM processes are in place. Some banks have not fully integrated into the system. From our finding, it is imperative for the central bank of Nigeria (CBN) to further strengthen their supervisory control measure, on the commercial banks, to ensure more efficient implementation of information security risk management across all commercial banks. Banking, academic and consulting institutions, information security experts and other professional bodies can also contribute to educate the community about the importance of cyber security threats affecting the society especially the banking industry.

6.2 Conclusion

This study investigated factors influencing the implementation of information security risk management among Nigerian Commercial Banks. It was discovered that management support affects the quality of information security risk assessment in the banking industry. Furthermore, it explained that the quality of information security risk assessments imparts the existence of management itself. It was also discovered that technical expert's support influences information security risks assessment in the commercial banks because their involvement in competent information system experts to create seamless IS risk management assessment, and the IT security practitioners in the organizational support uses the risk management process to identify and assess potential IS risks. More so, it was discovered that the use of the IT systems and data according to an organization's policies, guidelines, and rules of behaviour is critical to mitigating risk and protecting the organization's IT resources.

6.3 Recommendations

Based on the findings of this study the following are hereby suggested.

- Management should track the degree of adherence to organization's policies, guidelines, and rules of behaviour. This is critical because it possess that capacity to mitigate risk by protecting the organization's IT resources.
- It is also recommended that finance should be considered in IS risk assessment, because it is essential for the long-term growth of the organization and regular IT risk assessment can help the company eliminate unnecessary security spending.
- It is suggested that information system experts should endeavour to apply the use of the risk management process to identify and assess potential IS risks.
- The management team should enhance their support roles in the areas of support decision making in IS risk management, integrating risk management into decision-making process to create efficiency in procedure and control in common risk management and the management offers support in developing training programs, supporting quality management, formulating objectives and strategies for IS risk assessment.

6.4 Limitations of the Study

Despite all efforts invested to make this work fault-free there are still some short comings that were encountered.

The scope of this study was limited to commercial banks staff in Nigeria whose perspective might differ from that of the customers which impedes the generalization of the result when considering the views of customers. More importantly, the trajectories of factors influencing information security risk assessment in this study were centred on management support, user security awareness, IT expert support and funding. However, there could be other factors from the end customers or the business climate of the country which could contribute to information security risk assessment which are not accounted for in this study. However, despite all odds, the findings of this study will still be able to provide answers to the research questions raised.

6.5 Suggestions for Further Studies

Though attempts have been made in this study to establish the factors influencing the implementation of information security risk management among Nigerian Commercial Banks. However, the following are suggested for further research.

- A cross-sectional design with a broader sample size could be adopted in subsequent studies.
- This study considered Nigerian banks alone, subsequent studies could try out a comparative investigation of some African banks' information security risk management. This could go a long way in the generalization of the result. Other promising variables could be included as predictors of information security risk management using a regression model.

The ultimate objective of this research study is to explore and discuss the motivating factors influencing the implementation of information security risk management in the case of Nigerian Commercial Banks. The banking sector is always a prime target of attack by criminals, both online and offline. To an extent, this objective has been partially achieved. The study focused only on the information security side of implementing risk management, and not on the main banking business of lending and accepting deposits from the public. There is to emphasize that an area of further research is necessary, because commercial banks in Nigeria have not fully embraced the ISRM practices. Nigeria is a developing country, and at the same time struggling to develop a more conducive business investment environment to attract both national and international investors.

REFERENCES:

Anderson, R. & Moore, T. (2006). The Economics of Information Security" Science USA, Vol. 314, No. 5799, pp. 610–613.

Alali, M., Almogren, A., Hassan, M. M., Rassan, I. A., & Bhuiyan, M. Z. A. (2018). Improving risk assessment model of cyber security using fuzzy logic inference system. Computers & Security, 74, 323-339.

Babatunde D. A., (2014). The determinant of information security practices towards organizational performance in the banking sector: evidence from Nigeria. International *Journal of Business and Management; Vol. 9, No. 7.*

Bhattacherjee, A., (2012). Social Science Research: Principles, Methods, and Practices. Scholar Commons, University of Florida, USA.

Bryman, A., (2015). Social Research Methods - 5th Edition. Oxford University Press.

Bouveret, A. (2018). Cyber risk for the financial sector: A framework for quantitative assessment. International Monetary Fund.

Bekhet, A. K., & Zauszniewski, J. A. (2012). Methodological triangulation: An approach to understanding data. *Nurse researcher*.

Bergström, E., Lundgren, M., & Ericson, Å. (2019). Revisiting information security risk management challenges: a practice perspective. Information & Computer Security.

Canavan, S., (2004). An Information Security Policy Development Guide for Large Companies" SANS Institute. Journal of Advanced Nursing, UK, Vol. 20, pp.716-721. CBN (2018). Financial Stability Report December 2018 Central Bank of Nigeria (CBN), Statistical Bulletin (2019), Abuja

Charitoudi, K., & Blyth, A., (2013). A Socio-Technical Approach to Cyber Risk Management and Impact Assessment. Journal of Information Security, 4(1), 33-41.

Clegg, C., Robinson, M., Davis, M., Bolton, L., Pieniazek, R., & McKay, A. (2017). Applying organizational psychology as a design science: A method for predicting malfunctions in socio-technical systems (PreMiSTS). Design Science, 3, E6. doi:10.1017/dsj.2017.4

Dhillon, G., (2013). Managing and Controlling Computer Misuse, Vol. 7, No. 4, pp. 171- 175,

Doherty. N., and Fulford, H., (2005). Do Information Security Policies Reduce the Incidence of Security Breaches: An Exploratory Analysis, Information Resources Management Journal, Vol. 18, No. 2, pp. 21-39.

Dapp, T., Slomka, L., AG, D. B., & Hoffmann, R. (2014). Fintech–The digital (r) evolution in the financial sector. Deutsche Bank Research, 11, 1-39.

Dabari, I. J., & Saidin, S. Z. (2015). Determinants influencing the implementation of enterprise risk management in the Nigerian banking sector. International Journal of Asian Social Science, 5(12), 740-754.

Ezeoha, A. E (2005), Regulating Internet Banking in Nigeria, Problem and Challenges-Part1, Journal of Internet Banking and Commerce, December 2005, Vol. 10, No. 3. Retrieved 5th August, 2006 from http://www.arraydev.com/commerce/jibc/

Fasilat A. S., & Satirenjit, K. J., (2021). Assessment of Top Management Commitment and Support on IS Risk Management Implementation in the Business Organization, Risk Management. www.intechopen.com/chapters/75344

Girma, A., & Lemma, L., (2020). Human Factors Influence in Information Systems Security: Towards a Conceptual Framework. Proceedings of the 2nd African International Conference on Industrial Engineering and Operations Management Harare, Zimbabwe, December 7-10, 2020

Gitau, I. N., (2018). Factors hindering integration of physical access control and cyber security in the banking sector in Kenya. Unpublished research Dissertation submitted for the award of Master of Science Degree in Information Technology Management, University of Nairobi

Gana, N. N., Abdulhamid, S. I. M., & Ojeniyi, J. A. (2019). Security risk analysis and management in banking sector: A case study of a selected commercial bank in Nigeria.

Gaillard, A. (2021). Cybersecurity Challenges and Governance Issues in the Cyberspace' When Stronger Passwords Are Not Enough: Governing Cyberspace in Contemporary African Nations' Case Study: Can South Africa and Nigeria Secure Cyberspace without a Lock. Available at SSRN 3877526.

Gupta, M., Chaturvedi, A., & Mehta, S. (2011). Economic analysis of trade-offs between security and disaster recovery. Communications of the Association for Information Systems, 28(1), 1.

Hussein, A. (2009). The use of triangulation in social sciences research. Journal of comparative social work, 4(1), 106-117.

Huyghue, B. D. (2021). Cybersecurity, Internet of Things, and Risk Management for Businesses (Doctoral dissertation, Utica College).

Han, D., Dai, Y., Tianlin Han, & Dai, X., (2015). Explore Awareness of Information Security:

Insights from Cognitive Neuro-mechanism. Computational Intelligence and Neuroscience, 1- 11.

Hinde, S., (2002). Security Surveys Spring Crop. Computers and Security", Vol. 21, No. 4, pp. 310-321.

Hone, K. & Eloff, J., (2002). What makes an Effective Information Security Policy", Network Security, Vol. 20, No. 6, pp. 14-16, 2002.

Hubbard F.T., Yu-chieh, L., Zahs D., & Hu M., (2016). Sample Design. Cross-Cultural Survey Guidelines © Copyright 2016 International Standards Organization, ISO/IEC 27002," 2013 International Standards Organization, ISO/IEC 27002," 2016.

ISO/IEC 27005:2018. Information Technology—Security Techniques—Information Security Risk Management; ISO Standard: Geneva, Switzerland, 2018

Kuzminykh, Ievgeniia & Ghita, B.V. & Sokolov, Vladimir & Bakhshi, Taimur. (2021). Information Security Risk Assessment. 1. 602-617. 10.3390/encyclopedia1030050.

Kombo, D. K., & Tromp, D. L. (2011). Proposal and Thesis Writing; an Introduction. Nairobi: Paulines Publications Africa.

Kothari, C. R., (2011). Research Methodology; Methods and Techniques. New Delhi: New Age International Publishers.

Lubua, E. W., & Pretorius, P. D., (2019). Ranking Cybercrimes based on their impact to organizations' welfare. THREAT Conference Proceedings (pp. 1-11). Johannesburg: THREAT Conference Proceedings.

Lundgren, B., & Möller, N. (2019). Defining information security. Science and engineering ethics, 25(2), 419-441.

Machogu, J. M., (2019). Information security management practices and risk exposures among commercial banks in Kenya. Unpublished research project for the award of the degree of master's in business administration (MBA), school of business, university of Nairobi.

Malatji, M., Von Solms, S. and Marnewick, A., 2019. Socio-technical systems cybersecurity framework. Information & Computer Security.

Markon, K. E., Chmielewski, M., & Miller, C. J. (2011). The reliability and validity of discrete and continuous measures of psychopathology: A quantitative review. *Psychological Bulletin, 137*(5), 856–879. https://doi.org/10.1037/a0023678

Martin, K., & Acuna, C., (2002). SPSS for Instructional Researchers. Lewisburg, Pennsylvania: Bucknell University Press.

Porra, J., & Hirschheim, R. (2007). Enid Mumford's Contribution to Information Systems Theory and Theoretical Thinking: Introduction to the Special Issue. *Journal of the Association for Information Systems*, *8*(9), 30.

Obeidat I., & Mughaid A., (2019). Implementing Factors of Information Security in Governmental Organizations of Jordan. ICDS 2019: The Thirteenth International Conference on Digital Society and eGovernments

Östlund, U., Kidd, L., Wengström, Y., & Rowa-Dewar, N., (2011). Combining qualitative and quantitative research within mixed method research designs: a methodological review. International Journal of Nursing Studies 48(3):369-83.

Omodunbi, B. A., OM, O., Adeyanju, I. A., Sobowale, A. A., Nnamdi, O., Adebimpe, E., & Adanigbo, O. O. CYBER SECURITY THREATS IN THE ERA OF COVID-19 PANDEMIC: A CASE STUDY OF NIGERIA SYSTEM.

Pramanik, S., Samanta, D., Vinay, M., & Guha, A. (Eds.). (2022). Cyber Security and Network Security. John Wiley & Sons.

Shahri, A. B., & Mohanna, S., (2016). The Impact of the Security Competency on "Self-efficacy in Information Security" for Effective Health Information Security in Iran. The Advances in Intelligent Systems and Computing, 445, 51-65.

Singh, R., & Malpani, A., (2018). To Investigate the Factors Affecting Security of Management information System in Financial Institutions. www.researchgate.net/publication.

Siponen, M. T., (2001). Information Systems Audit and Control Association, "Critical elements of information security program success.

Simon, M. K., & Goes, J. (2013). Assumptions, limitations, delimitations, and scope of the study.

Siponen, M., & Vance, A. (2010). Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations. MIS Quarterly, 34(3), 487–502. https://doi.org/10.2307/25750688.

Tryfonas, T., (2001). Embedding Security Practices in Contemporary Information systems Development Approaches" Information Management & Computer Security, Vol. 9, No. 4, pp. 183-197,

Tooze, A. (2019). Why central banks need to step up on global warming. Foreign Policy, 20.

Ugwuanyi, S., Okechukwu, A., Prince, O., Okechukwu, N., & Irvine, J. (2020, August). Cybercrimes in Southern Nigeria and survey of IoT implications. In 1st IEEE Multi-Conference Technical Series (MCTS) 2020.

Ugbe, U. M. (2021). Exploring the Security Measures to Reduce Cyberattacks within the Nigerian Banking Sector: A Qualitative Inquiry (Doctoral dissertation, Capella University).

Varga, S., Brynielsson, J., & Ulrik F., (2021). Cyber-threat perception and risk management in the Swedish financial sector. Journal of computers & security 105 (2021) 102239

Wright, J., Dawson Jr, M. E., & Omar, M. (2012). Cyber security and mobile threats: The need for antivirus applications for smartphones. Journal of Information Systems Technology and Planning, 5(14), 40-60.

Wang, V., Nnaji, H., & Jung, J. (2020). Internet banking in Nigeria: Cyber security breaches, practices and capability. International Journal of Law, Crime and Justice, 62, 100415.

Yeo, A. C., & Rahim, M. M., (2016). Understanding Factors Affecting Success of Information Security Risk Assessment: The Case of an Australian Higher Educational Institution. Industrial Management & Data Systems (106:3), pp. 345-361.

Zio, E. (2018). The future of risk assessment. Reliability Engineering & System Safety, 177, 176-190.

Zoto, E., Kowalski, S., Lopez-Rojas, E. A., & Kianpour, M. (2018). Using a socio-technical Systems Approach to design and support systems thinking in cyber security education. 4th International Workshop on Socio-Technical Perspective in IS development (STPIS'18) (pp. 123-128). Tallinn] - Estonia: 4th International Workshop on Socio-Technical perspective in IS development (STPIS'18).

APPENDICES

APPENDIX I: DECLARATIONS

Dear Respondent,

Our names are Okojie Bukky E. and Gabriel Aghaunor, students at Lulea University of Technology, Department of computer science, Electrical and Space Engineering in Sweden. We are conducting a research entitled **"FACTORS INFLUENCING THE IMPLEMENTATION OF INFORMATION SECURITY RISK MANAGEMENT. A CASE STUDY OF NIGERIAN COMMERCIAL BANKS".** We are kindly requesting you to provide information in regard to this topic. A questionnaire here below has been designed and we are requesting you to provide information to address the research objectives of the study.

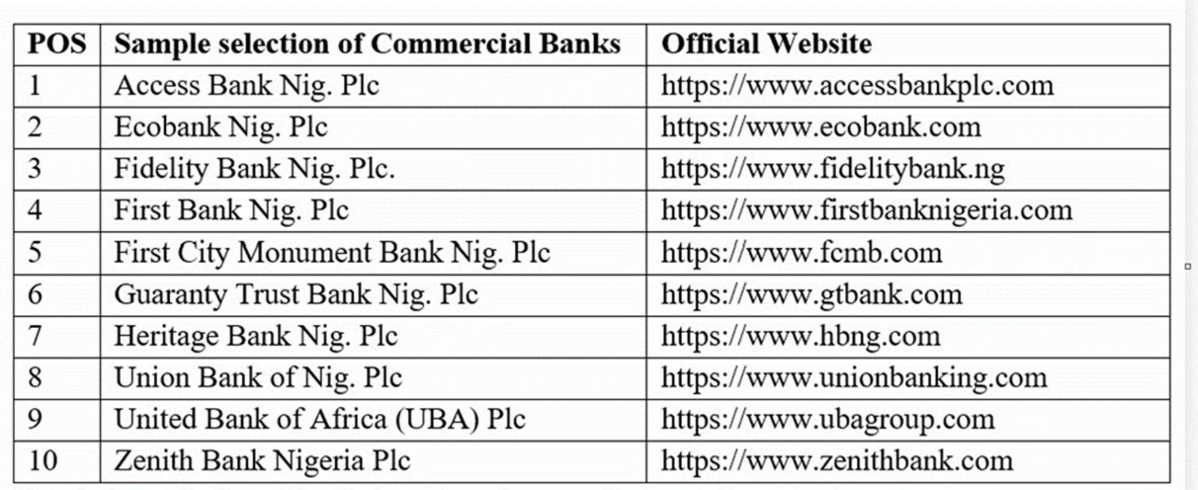
Please note that this study is an academic research and the information provided will be treated in strict confidentiality.

Your assistance is highly appreciated.

Okojie Bukky E. …………….………….. ……………………..
Signature **Date**

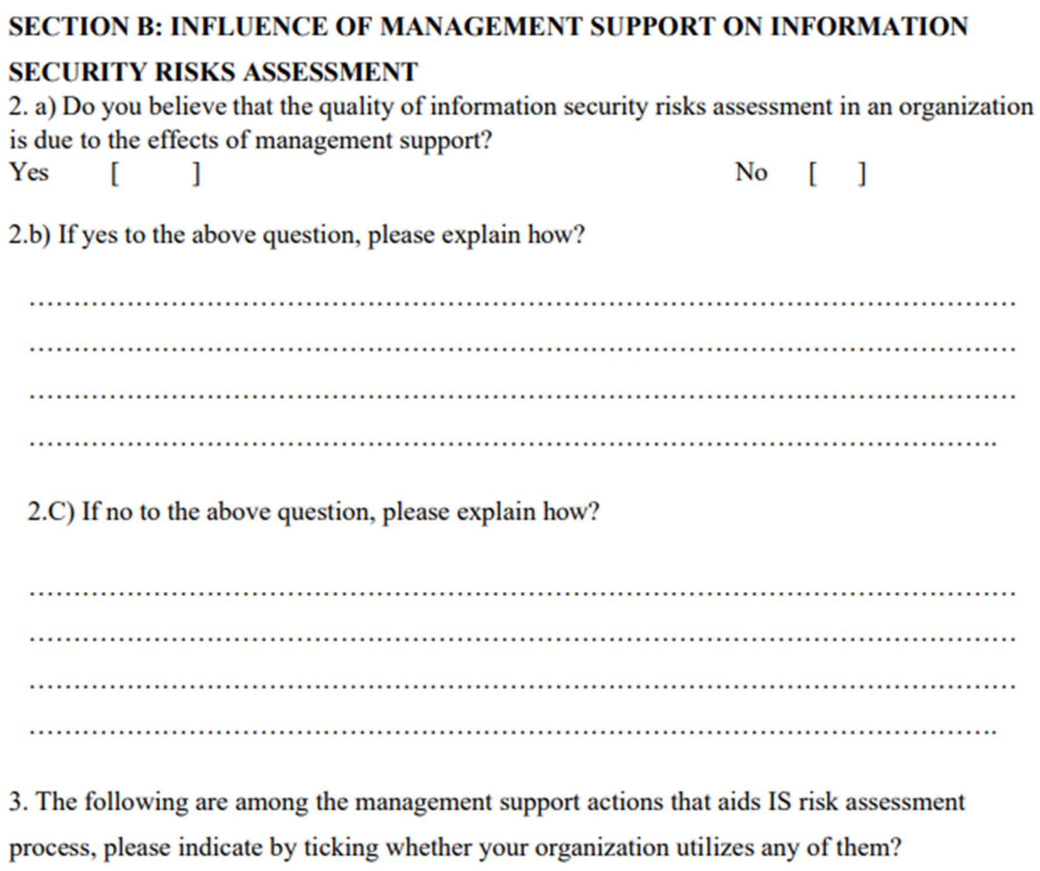
Gabriel Aghaunor …………….………….. ……………………..
Signature **Date**

APPENDIX II: TARGET POPULATION



POS	Sample selection of Commercial Banks	Official Website
1	Access Bank Nig. Plc	https://www.accessbankplc.com
2	Ecobank Nig. Plc	https://www.ecobank.com
3	Fidelity Bank Nig. Plc.	https://www.fidelitybank.ng
4	First Bank Nig. Plc	https://www.firstbanknigeria.com
5	First City Monument Bank Nig. Plc	https://www.fcmb.com
6	Guaranty Trust Bank Nig. Plc	https://www.gtbank.com
7	Heritage Bank Nig. Plc	https://www.hbng.com
8	Union Bank of Nig. Plc	https://www.unionbanking.com
9	United Bank of Africa (UBA) Plc	https://www.ubagroup.com
10	Zenith Bank Nigeria Plc	https://www.zenithbank.com

APPENDIX III



SECTION B: INFLUENCE OF MANAGEMENT SUPPORT ON INFORMATION SECURITY RISKS ASSESSMENT

2. a) Do you believe that the quality of information security risks assessment in an organization is due to the effects of management support?

Yes [ ] No [ ]

2.b) If yes to the above question, please explain how?

…………………………………………………………………………………………………

…………………………………………………………………………………………………

…………………………………………………………………………………………………

……………………………………………………………………………………………….

2.C) If no to the above question, please explain how?

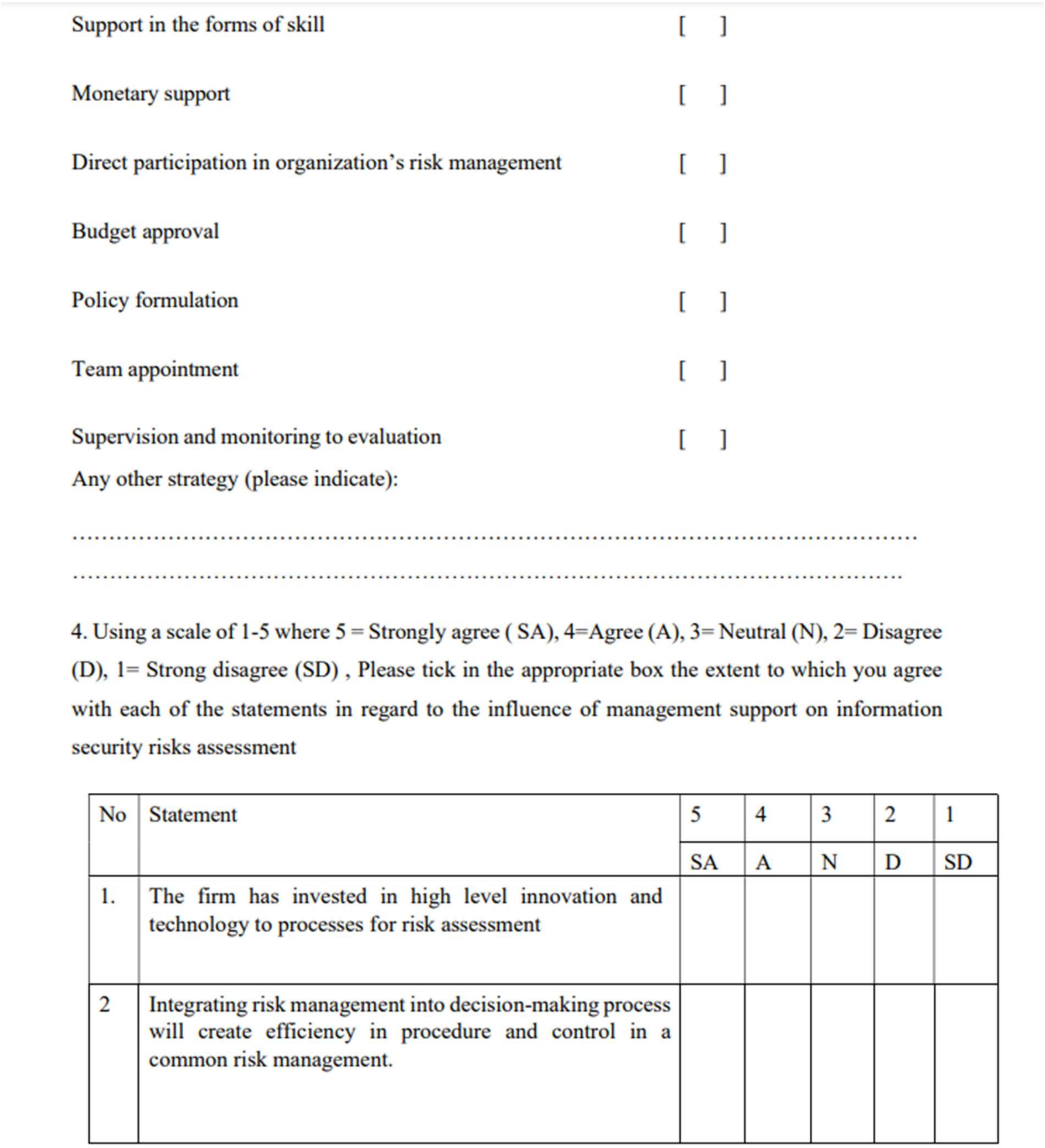
…………………………………………………………………………………………………

…………………………………………………………………………………………………

…………………………………………………………………………………………………

……………………………………………………………………………………………….

3. The following are among the management support actions that aids IS risk assessment process, please indicate by ticking whether your organization utilizes any of them?



Support in the forms of skill [ ]

Monetary support [ ]

Direct participation in organization's risk management [ ]

Budget approval [ ]

Policy formulation [ ]

Team appointment [ ]

Supervision and monitoring to evaluation [ ]

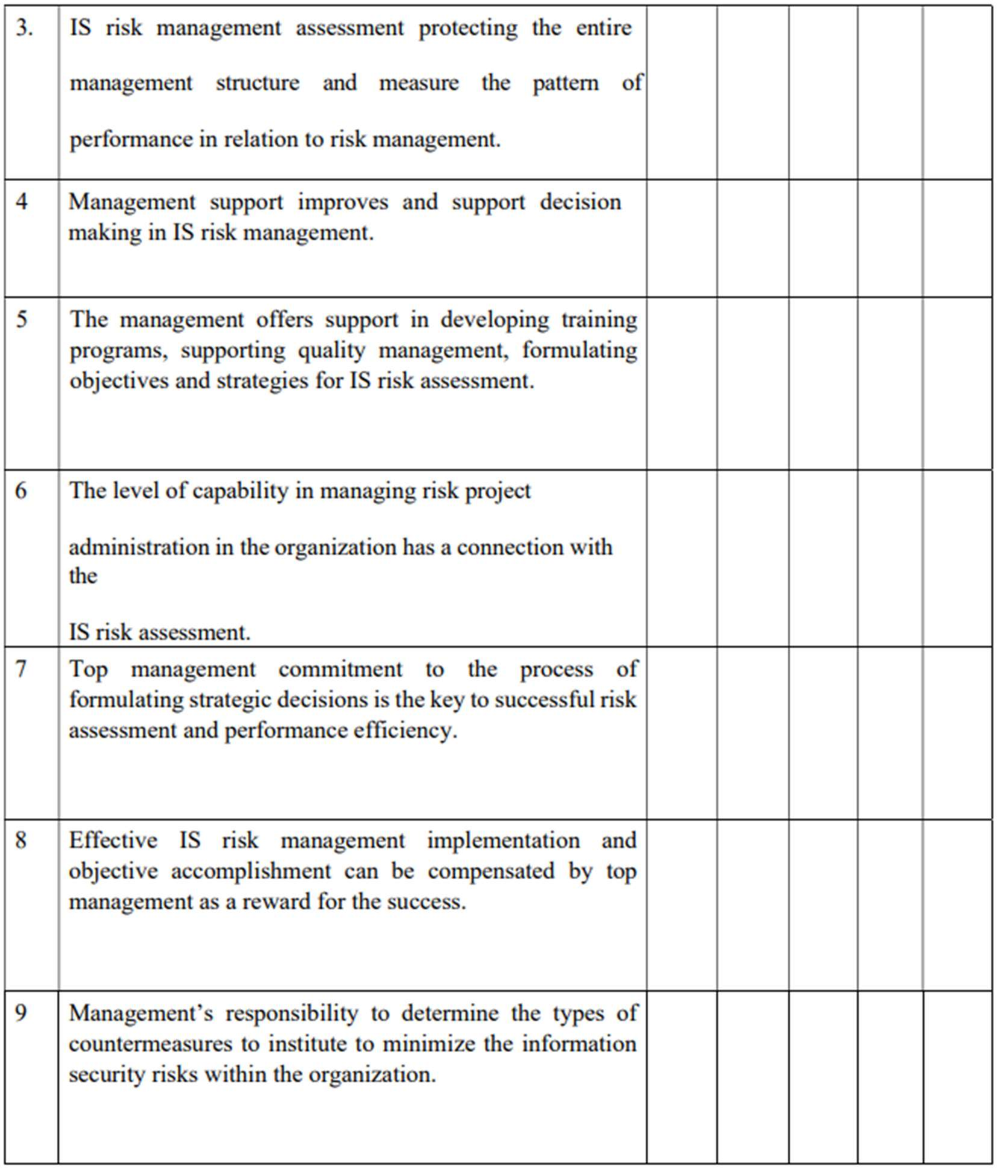
Any other strategy (please indicate):

……………………………………………………………………………………………………

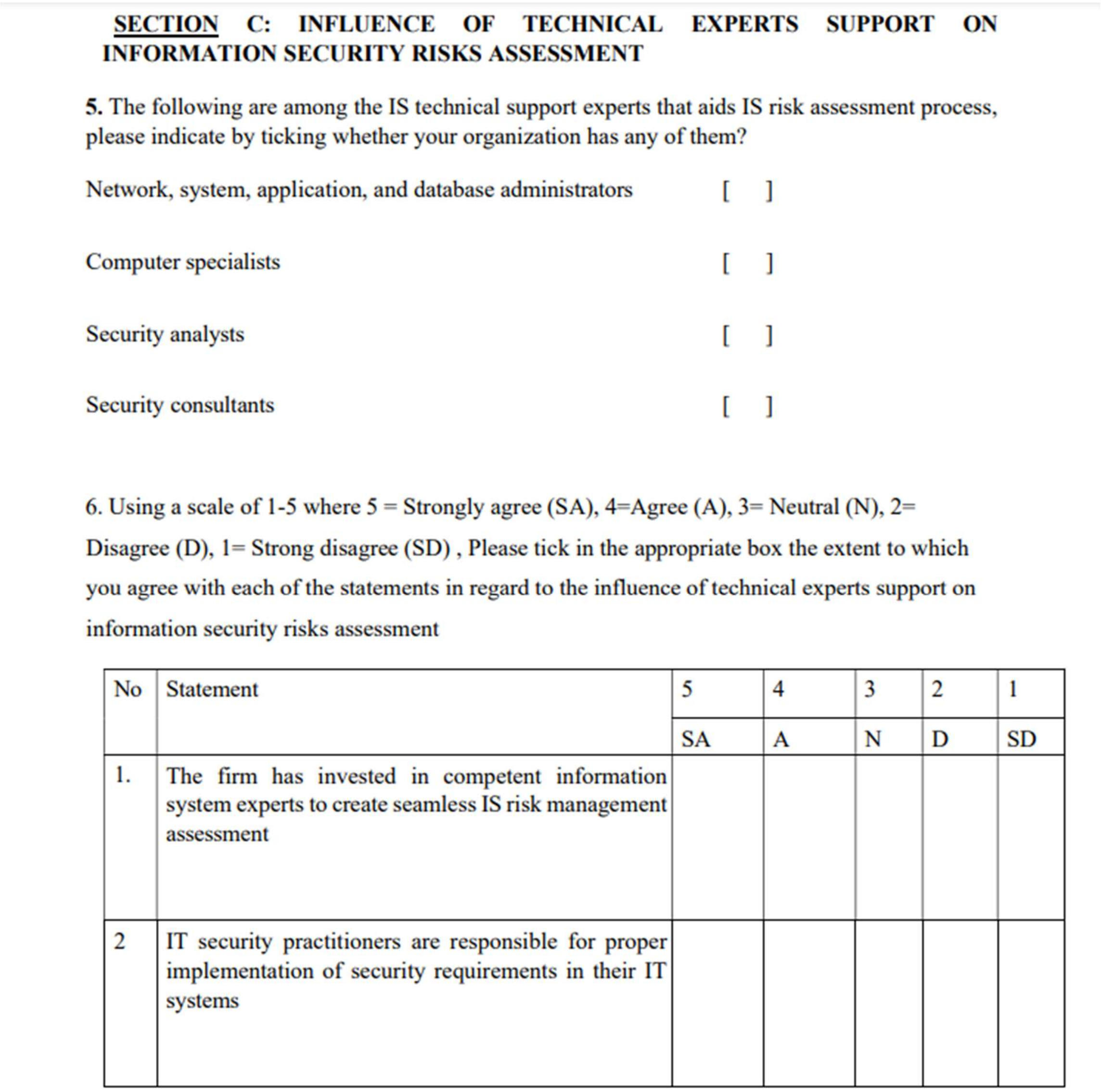
……………………………………………………………………………………………………

4. Using a scale of 1-5 where 5 = Strongly agree (SA), 4=Agree (A), 3= Neutral (N), 2= Disagree (D), 1= Strong disagree (SD) , Please tick in the appropriate box the extent to which you agree with each of the statements in regard to the influence of management support on information security risks assessment

No	Statement	5	4	3	2	1
		SA	A	N	D	SD
1.	The firm has invested in high level innovation and technology to processes for risk assessment					
2	Integrating risk management into decision-making process will create efficiency in procedure and control in a common risk management.					



3.	IS risk management assessment protecting the entire management structure and measure the pattern of performance in relation to risk management.					
4	Management support improves and support decision making in IS risk management.					
5	The management offers support in developing training programs, supporting quality management, formulating objectives and strategies for IS risk assessment.					
6	The level of capability in managing risk project administration in the organization has a connection with the IS risk assessment.					
7	Top management commitment to the process of formulating strategic decisions is the key to successful risk assessment and performance efficiency.					
8	Effective IS risk management implementation and objective accomplishment can be compensated by top management as a reward for the success.					
9	Management's responsibility to determine the types of countermeasures to institute to minimize the information security risks within the organization.					



SECTION C: INFLUENCE OF TECHNICAL EXPERTS SUPPORT ON INFORMATION SECURITY RISKS ASSESSMENT

5. The following are among the IS technical support experts that aids IS risk assessment process, please indicate by ticking whether your organization has any of them?

Network, system, application, and database administrators [ ]

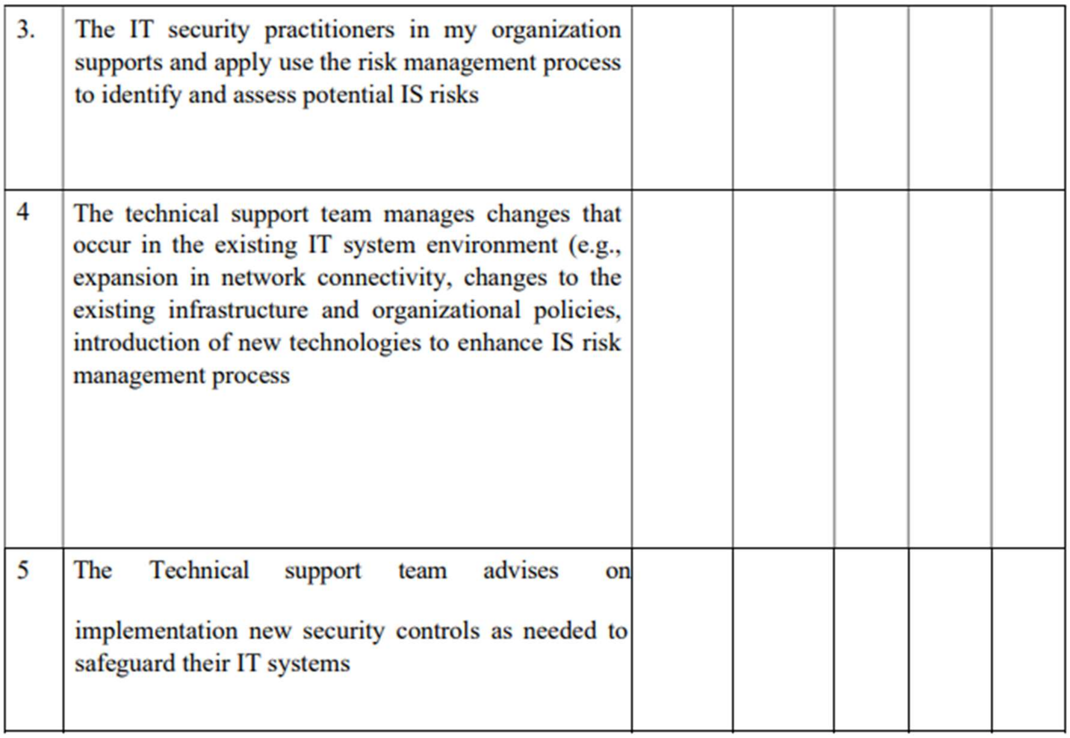
Computer specialists [ ]

Security analysts [ ]

Security consultants [ ]

6. Using a scale of 1-5 where 5 = Strongly agree (SA), 4=Agree (A), 3= Neutral (N), 2= Disagree (D), 1= Strong disagree (SD) , Please tick in the appropriate box the extent to which you agree with each of the statements in regard to the influence of technical experts support on information security risks assessment

No	Statement	5	4	3	2	1
		SA	A	N	D	SD
1.	The firm has invested in competent information system experts to create seamless IS risk management assessment					
2	IT security practitioners are responsible for proper implementation of security requirements in their IT systems					

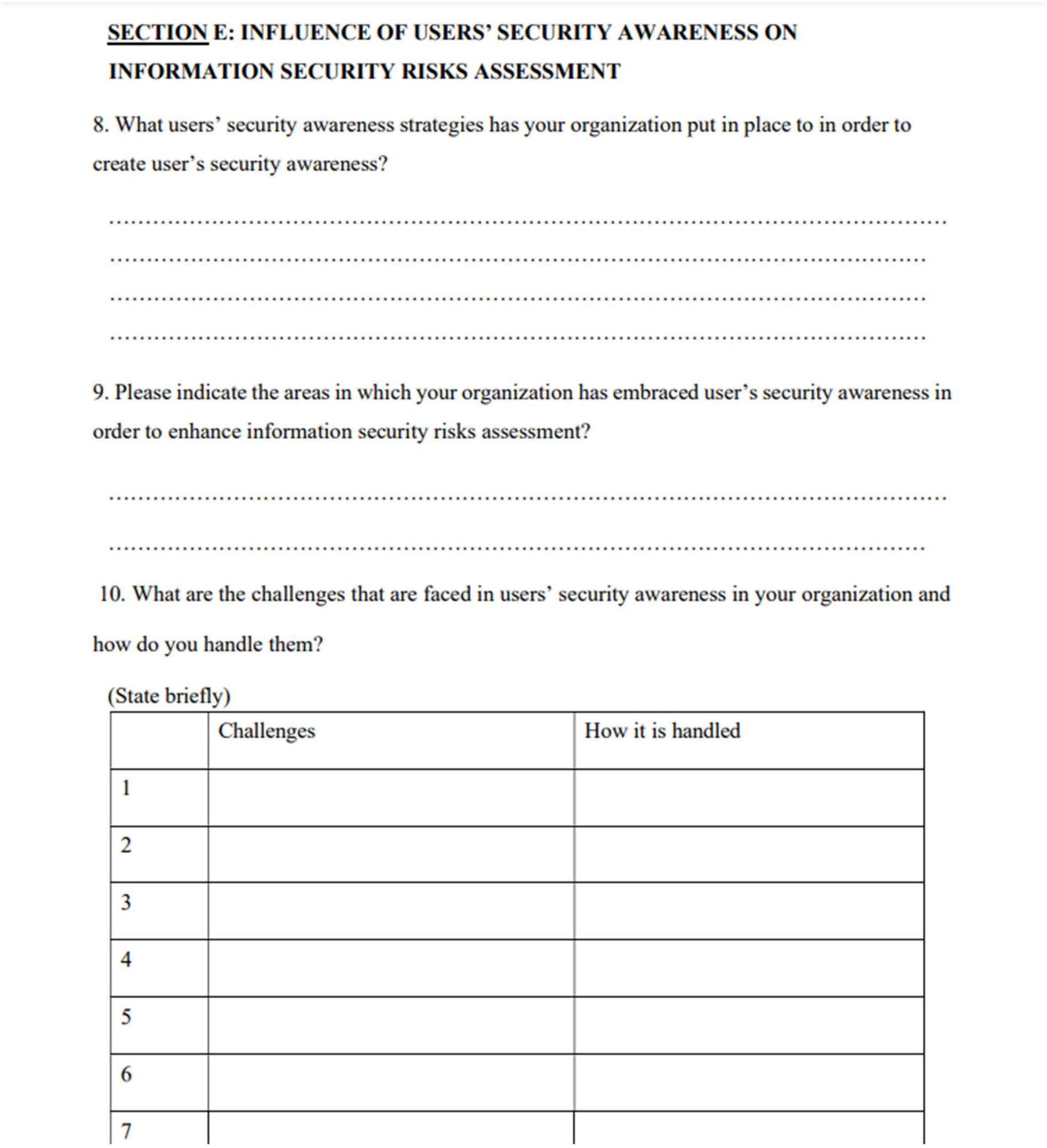


3.	The IT security practitioners in my organization supports and apply use the risk management process to identify and assess potential IS risks					
4	The technical support team manages changes that occur in the existing IT system environment (e.g., expansion in network connectivity, changes to the existing infrastructure and organizational policies, introduction of new technologies to enhance IS risk management process					
5	The Technical support team advises on implementation new security controls as needed to safeguard their IT systems					

SECTION D: INFLUENCE OF FUNDING ON INFORMATION SECURITY RISKS ASSESSMENT

7. Using a scale of 1-5 where 5 = Strongly agree (SA), 4=Agree (A), 3= Neutral (N), 2= Disagree (D), 1= Strong disagree (SD) , Please tick in the appropriate box the extent to which you agree with each of the statements in regard to the influence of funding on information security risks assessment

No	Statement	5	4	3	2	1
		SA	A	N	D	SD
1.	The lack of sufficient security budgets is often an obstacle to achieving the desired level of information security protection assessment					
	Regular IT risk assessment can help your company eliminate unnecessary security spending.					
	Our Finance department actively involved in collaboration with IT leadership in developing and implementing policies and procedures that support IS risk assessment					
	The involvement of Finance in IS risk assessment is essential for the long-term growth of the organization					



SECTION E: INFLUENCE OF USERS' SECURITY AWARENESS ON INFORMATION SECURITY RISKS ASSESSMENT

8. What users' security awareness strategies has your organization put in place to in order to create user's security awareness?

……………………………………………………………………………………………………

…………………………………………………………………………………………………

…………………………………………………………………………………………………

…………………………………………………………………………………………………

9. Please indicate the areas in which your organization has embraced user's security awareness in order to enhance information security risks assessment?

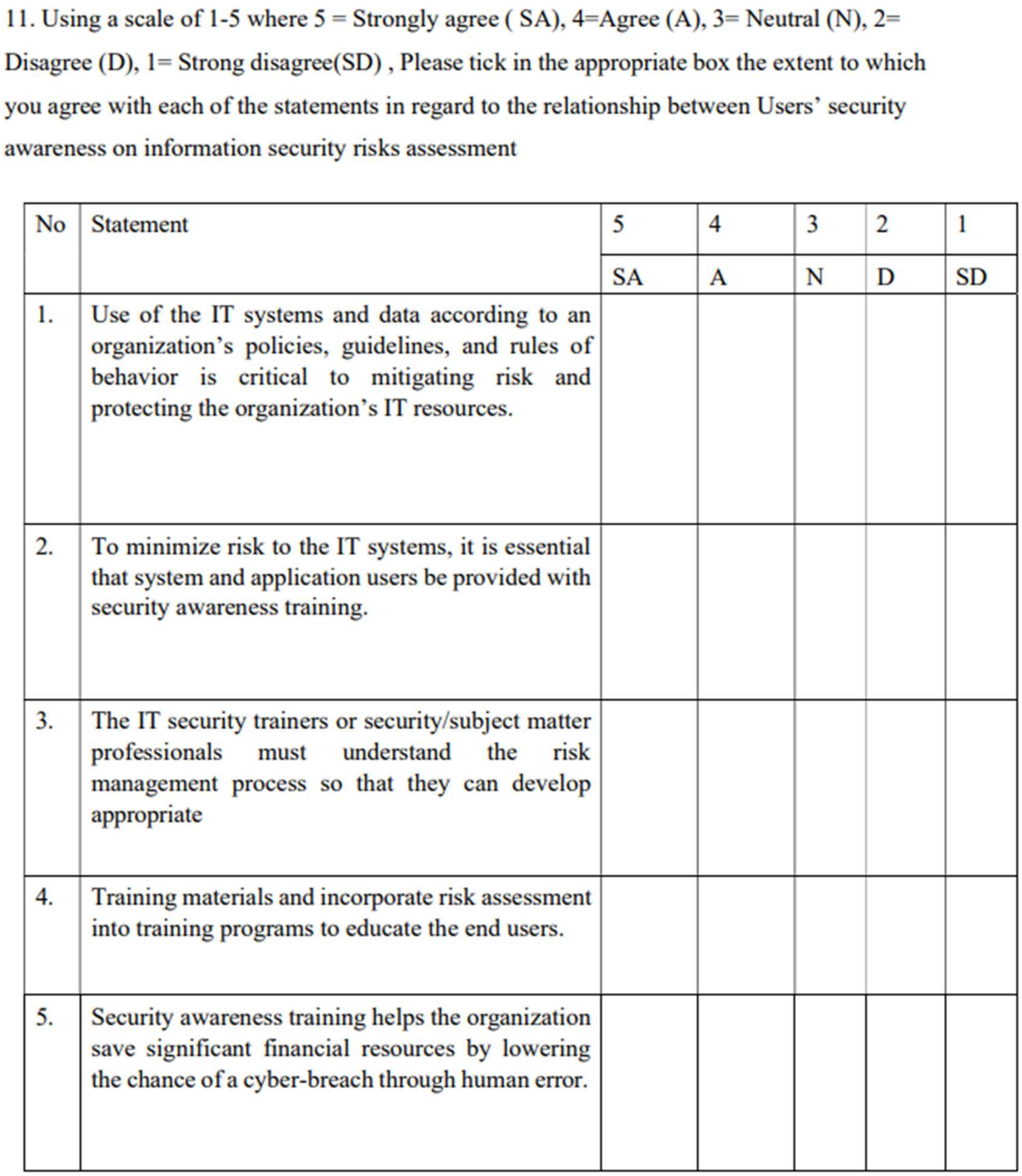
……………………………………………………………………………………………………

…………………………………………………………………………………………………

10. What are the challenges that are faced in users' security awareness in your organization and how do you handle them?

(State briefly)

	Challenges	How it is handled
1		
2		
3		
4		
5		
6		
7		



11. Using a scale of 1-5 where 5 = Strongly agree (SA), 4=Agree (A), 3= Neutral (N), 2= Disagree (D), 1= Strong disagree(SD) , Please tick in the appropriate box the extent to which you agree with each of the statements in regard to the relationship between Users' security awareness on information security risks assessment

No	Statement	5	4	3	2	1
		SA	A	N	D	SD
1.	Use of the IT systems and data according to an organization's policies, guidelines, and rules of behavior is critical to mitigating risk and protecting the organization's IT resources.					
2.	To minimize risk to the IT systems, it is essential that system and application users be provided with security awareness training.					
3.	The IT security trainers or security/subject matter professionals must understand the risk management process so that they can develop appropriate					
4.	Training materials and incorporate risk assessment into training programs to educate the end users.					
5.	Security awareness training helps the organization save significant financial resources by lowering the chance of a cyber-breach through human error.					

APPENDIX IV:

Qualitative Approach of Interview Guide

General Questions:

1. Is it acceptable if I can include your name in the thesis?

2. What is your name sir/madam?

3. Please can tell me about your position in the bank?

4. Can you tell me how long have you worked in the bank?

5. What is your level of working experience?

6. What is your educational qualification?

Cyber-Risk Measurement

7. How would you measure risk assessment within your bank? And which criteria would you use to measure risk?

Influence of Management Support

8. Do you believe that the quality of information security risks assessment in an organization is because of management support?

9. What are the management support action that aids information security risk management process?

10. What are the information security policies guiding the operation of your bank?

11. How has the management influence the process of information security risk management implementation within your bank?

12. Why do you think information assets need to be identified within the bank before classification?

Influence of Technical Expert Supports

13. What has the technical experts contributed so far in improving the information security posture of your bank?

Influence of Users' Security Awareness

12. What are the challenges that are faced in users' security awareness in your organization and how do you handle them?

13. What are the most frequent cyber risks that your bank faces?

17. How can these risks be controlled or mitigated?

18. Conclusion. What change do you hope can take place in the banking industry to improve ISRM implementation?