Managing Information Security while maintaining Organizational Agility

Temitayo Eniola Adetona

Department of Computer and Systems Sciences

Degree project 30 HE credits

Computer and Systems Sciences

Degree project at the master level

Spring term 2023

Supervisor: Gideon Mekonnen Jonathan Reviewer: Lazar Rusu

Stockholm University

Abstract

An organization's ability to succeed depends on the Confidentiality, Integrity, and Availability of its information. This implies that the organization's information and assets must be secured and protected. However, the regular occurrence of threats, risks, and intrusions could serve as a barrier to the security of this information. This has made the management of Information security a necessity. Organizations are then trying to be more agile by looking for ways to identify and embrace opportunities swiftly and confront these risks more quickly. Very little research has examined the relationships between Organizational Agility and Information Security. Hence, this study aims to investigate the management of Information Security in organizations while maintaining agility and highlighting the challenges encountered, and also addresses the research question: *How do organizations manage information security while maintaining organizational agility?*

The research strategy used is the Case Study, and the data collection methods used are semi-structured interviews and documents. The interview was conducted in a financial institution in Nigeria with seven security specialists, and documents were obtained from the company's website to help gain insights into the services and products offered. Thematic analysis was the data analysis method chosen. The findings revealed eighteen measures in which Information Security can be managed while maintaining Organizational Agility. Part of the identified measures are similar to those identified in previous research, while new measures are also discovered. Furthermore, these identified measures will be useful for other organizations, particularly financial institutions, to emulate in managing their Information Security and being agile while at it.

Keywords: Organizations, Information Security, Organizational Agility, Information Security Management.

Synopsis

Background

Information technology systems are used to communicate and process information for organizational and operational procedures; hence, this data must be protected. Information security consists of three components: Confidentiality, Integrity, and Availability. With the dependence of organizations on Information security, breaches are also on the increase, which could negatively affect how those organizations operate. Information Security Management is therefore necessary. Organizational agility refers to a company's capacity to react quickly and modify its operations in response to changing conditions. Despite organizational agility's impact on information security, businesses are continually worried about maintaining it in the face of changing dangers and breaches.

Problem

Organizations still face some challenges managing their information security while maintaining agility. Information security management and organizational agility have each been studied separately in previous studies. Few in-depth analyses of their relationship have been conducted. Hence, the reason is to better understand how businesses handle information security while maintaining agility.

Research Question

The aim of this study is to investigate the management of Information Security in organizations while maintaining organizational agility. The study's research question, which tries to address the already described research problem, is: *How do organizations manage information security while maintaining organizational agility?*

Method

The research strategy selected for this study is the Case Study. This took place in one of the financial organizations in Nigeria. Semi-structured interviews and Documents obtained from the company's website are the data collection methods. Non-probability sampling and purposive sampling methods were used in selecting the participants. The chosen analysis technique was the Thematic Analysis.

Result

The Thematic Analysis of the collected data revealed eighteen measures in which Information Security can be managed in the organization together with agility. The eighteen sub-themes were further categorized into eight themes. Sixteen out of the eighteen measures have been discussed in previous research. The newly identified measures are *Strong Legal Documents and Virtual Phone Networks – VPN,* and they are categorized under this theme of *Third-party authentication.*

Discussion

The objective of this study is to show how businesses manage information security while retaining agility. Some of the measures found are comparable to those found in earlier studies. There were newly discovered measures. Since the case study was only undertaken in one organization, these measures may not necessarily be applicable to all organizations. Due to the parallels in their modes of operation with the business utilized as the case study, the newly identified measures could also be helpful to other

organizations, primarily financial institutions. The participants were chosen based on their level of cybersecurity competence, and participation was optional.

Acknowledgment

I dedicate this thesis to God Almighty who has made it possible for me to see the completion of my master's program. My appreciation also goes to my husband and daughters for their immense support and understanding. I am thankful to my supervisor, Dr. Gideon Mekonnen Jonathan for his guidance, timely response, and feedback. My sincere gratitude also goes to all my lecturers in Computer and System Sciences department at Stockholm University for the great knowledge impacted on me. I want to specially thank my friend, Oluwakemi Aina for her support and the great role she played. Lastly, I want to appreciate the organization used as the case study, particularly the seven participants.

Table of Contents

List of Figures

List of Tables

List of Abbreviations

HVAC - Heating, Ventilation, and Air Conditioning
ICT - Information and Communication Technology
ISM – Information Security Management
ISMS – Information Security Management System
IT – Information Technology
VPN - Virtual Phone Network

1 Introduction

This chapter presents an introduction to the background of the study, the aim, the research problem, the research question, and the outline of the thesis.

1.1 Background

Information and communication technology (ICT) has an enormous impact on businesses today, which is indisputable. Moreover, most operational processes rely on ICT systems to send, process, and retain information, contributing to their importance. Hence, protecting the information these ICT systems process, store, and convey is essential.

Information security (Information Security) refers to the requirements to protect information, data, or assets considered valuable to the organization (Zaini et al., 2020). ISO/IEC 27000 (2014) standard further explained that to ensure ongoing business success and continuity and to reduce the effects of Information Security incidents, Information Security entails the application and administration of appropriate security measures that consider a wide variety of risks. Information Security has three components: confidentiality, integrity, and availability and according to Ma et al. (2008), even the most prominent business entity's survival may be in jeopardy if one or more of these goals were lost. Therefore, irrespective of the context in which a business operates, Information Security is vital to the success of an organization. Furthermore, this might be the foundation for creating business agility (Zaini et al., 2020). However, with the reliance of organizations on Information Security, breaches could be inevitable with significant consequences on the organization, which include financial loss and the integrity of the information and information system being compromised, amongst many others. This results in the need for Information Security Management (ISM).

ISM describes all the steps a company takes to address information availability, confidentiality, and integrity risks systematically. According to ISO/IEC 27000 (2014), an organization must effectively define, establish, maintain, and improve information security in order to protect its information assets, fulfill its goals, and preserve and improve its reputation and legal compliance. It is essential in all information service departments as a manner of operating, not only at the leadership/managerial level (Gunsberg et al., 2018). In order to be responsive, flexible, and have competitive advantages, an agile organization is expected to have efficient information access that can be used across divisions (Zaini et al., 2020).

Organizational agility (OA) is the capacity of a firm to adjust itself to unanticipated changes in the business environment by challenging the company to act swiftly in combining its technology, personnel, and management with communication infrastructure to adapt to such changes in quick and creative ways (Zaini & Masrek, 2013). Organizational Agility enables businesses to see opportunities rapidly, seize them, and deal with risks faster than their competitors. It is predicted that an ISM system, a system with centralized control that ensures access to accurate and timely information, will help boost organizational agility (Dehaghi, 2016). Also, with an effective ISM, Organizational Agility might be improved by ensuring that organizations are robust to internal and external threats (Zaini et al., 2020). Information transfer is frequent in agile businesses, necessitating serious security measures (Ebrahimian, 2012). Hence, it is necessary to get a deeper understanding of both entities – ISM and Organizational Agility separately, as well as understand the relationship between the two, which will help acquire more knowledge on how an organization can further boost its performance in terms of agility and security management.

Despite the advantages of using IT systems to increase Organizational Agility, organizations continue to be concerned about the risks connected with Information Security and the challenges faced while trying to control them using ISM such as limitation in finances, not having executive management support, and a shortage of qualified resources. Hence, it is crucial to understand how organizations use ISM to control risks while maintaining organizational agility highlighting the challenges encountered in the process.

1.2 Research Problem

Technology is now being used more frequently than ever to boost business performance which is demonstrated by the significant investment in advancing technology to replace legacy applications and boost agility. Information assets are subject to significant risks connected to information and cyber security. Because of this, an organization's ability to adapt is significantly impacted by the security of its information systems and other assets. Despite its importance, IT applications for agility may also have drawbacks (Zaini et al., 2020). Being able to effectively implement Information Security policies is one of the main challenges organizations face.

Several studies pointed out that it is no longer just a technological challenge to manage Information Security (von Solms and von Solms, 2004; Chang and Ho, 2006); it has to do with governance issues, and managerial considerations are crucial for organizational ISM. In addition, several issues with Information Security that firms throughout the world face, as highlighted by (Singh et al., 2013), are: support from top management; user awareness (training and education); vulnerability and risk management; issues with policies; internal threats; access control and identity management; organizational culture. Technology-driven security solutions can no longer address Information Security concerns due to today's increased global connectivity and quickly developing information technologies (Hall et al., 2011). To meet the difficulties and seize the opportunities created by the advancements in information technology, Caralli (2004) advised that instead of focusing on a technology-based information security strategy, firms should adopt an organizational-based strategy that considers a core set of organizational competencies.

However, little research has been conducted to establish the correlation between ISM and Organizational Agility and their impact on each other. According to Dehaghi (2016), only a few studies have been done on the relationship between information security management systems and Organizational Agility, but many more have been done on each factor separately. The two variables are connected. Also, Zaini et al. (2020) pointed out that a literature review revealed little research that concentrates on the connection between ISM and Organizational Agility. Although the development of agility as a dynamic capacity for gaining competitive advantage is frequently explored in literature, no theory currently incorporates information security strategy as a predictor for agility (Zaini et al., 2018). The correlations between Information Security and Organizational Agility were the subject of very few studies.

Dehaghi (2016) examined how information security management systems (ISMS) affect Organizational Agility in competition. It was envisioned by Luse et al. (2013) the role that information systems might play as crucial technological assets for achieving agility. Also, in research carried out by Li et al. (2006), it was pointed out that timely information sharing increases Organizational Agility by enhancing the reliability and efficiency of the production chain.

As a result, this study aims to investigate the management of Information Security in organizations while retaining organizational agility and highlighting the challenges encountered.

1.3 Research Question

The study's research question, which tries to address the previously described research problem, is:

How do organizations manage information security while maintaining organizational agility?

1.4 Thesis Outline

This research study consists of six chapters. The first chapter gives a broad introduction to the study, including the research problem, research question, and the aim of the study. The second chapter gives an overview of the extensive research done by previous researchers on the research topic, including ISM practices, Organizational Agility, and the relationship between ISM and Organizational Agility. The third chapter speaks on the choice of the research method, gives an overview of the different types of research strategies, data collection methods, data analysis methods, and eventually focuses on the methodologies that best suit the study as well as the research ethics. The fourth chapter, based on the data generated from the previous chapter, presents a discussion on the results obtained. Chapter five will discuss what the study entails, and Chapter six presents the conclusion, limitation and future research, originality, and significance as well as research quality.

2 Extended Background

This chapter gives an extended background of the research topic. It gives a detailed explanation of what an Information Security is, ISM practices, Organizational Agility and its types, the relationship between ISM and Organizational Agility, and the challenges related to ISM while maintaining Organizational Agility, all based on previous research.

2.1 Information Security and Information Security Management

Running a firm without its information systems functioning correctly and securely is frequently impossible or almost impossible (Ma et al., 2008). The practice of Information Security involves safeguarding data against unauthorized access and preventing unauthorized data access, use, modification, and destruction (Chopra & Chaudhary, 2020). Information Security is achieved typically by putting in place an appropriate set of controls that must be designed, implemented, monitored, reviewed, and updated, as needed, to ensure that the organization's specific security and business objectives are satisfied. Various frameworks, rules, and standards are presented by academics, and professional associations to secure enterprises' information assets. One of the most well-known initiatives on information security among them is the international standard ISO 17799 which has since been replaced by ISO 27002. This standard offers a reliable definition of Information Security and the steps that must be applied to attain it in a modern company (Ma & Pearson, 2005).

The effects of security breaches can be quite severe, given society's growing reliance on information technology (IT). In addition to financial losses, information system breaches can harm businesses through interruption of internal operations and communications, loss of prospective sales, loss of competitive advantage, and detrimental effects on a company's standing, goodwill, and trust. This has led to the need for ISM (Ma et al., 2008). ISM is the collection of procedures used to set up resources in a way that satisfies an organization's Information Security requirements. It is a component of the overall organization management system, which serves as the cornerstone for managing security risks (Ključnikov et al., 2019). Implementation of policies and guidelines for Information Security will allow organizations to stop threats, offering a solid level of defense for organizations. Such practice is also known as ISM (Zaini & Masrek, 2013). The three fundamental components of ISM are information availability, confidentiality, and integrity.

According to Ma and Pearson (2005), Information Security experts claim that ISO 17799 (now ISO 27002) is a suitable model for tackling ISM challenges and offers best practices on ISM. The standard includes 36 security practices across ten security dimensions (Appendix I). It serves as the foundation for self-evaluation, reviewing business partners' information security procedures, and conducting an unbiased assessment of ISM within the company. The standard identifies eleven organizational ISM domains, including asset management; compliance; communications and operations management; information system acquisition; access control; information security incident management; development, and maintenance; physical and environmental security; human resources security; and organizational information security. The overall goal of ISM is to increase the effectiveness and confidence of information services within or between organizations and their external business partners (Chang and Ho, 2006).

2.2 Information Security Management Practices

As was already established, Information Security primarily attempts to maintain information confidentiality, availability, and integrity. The transport, processing, and storage of information must be safeguarded holistically at all times for Information Security procedures to be effective. Given the variety of Information Security, managing Information Security can be a difficult task. However, by utilizing widely accessible best practices and standards, Information Security and its administration may be made far less scary (De Lange et al., 2016). The ISO/IEC 27001:2013 standard for ISM practices outlines the standards for establishing, implementing, running, monitoring, reviewing, maintaining, and upgrading an Information Security Management System (ISMS) that is documented.

There are fourteen (14) aspects of ISM practices listed by Zaini and Masrek (2013) and are based on security control procedures divided into three categories: organizational security, technical security, and physical and environmental security. There are also nine variables identified by Singh and Gupta (2013) that affect how ISM is implemented in small and medium-sized businesses, including security policy, asset classification and control, organizational security, personnel security, communications and operations management, physical security and environmental security, access control, business continuity management, and system development and maintenance.

ISM is likely one of the best predictors of Organizational Agility abilities. It strives to increase the effectiveness of business organizations' internal and external information services and IT infrastructure (Zaini & Masrek, 2013).

2.3 Organizational Agility

Gunsberg et al. (2018) defined *agility* as an organization's capacity to perceive or influence environmental change and act effectively in response to that change. Agility is a successful strategy or plan of action in a competitive market where client demand fluctuates quickly (Sindhwani et al., 2019). Businesses with excellent agility capabilities, according to (Walter, 2021), produce revenues 37% faster and make profits that are 30% higher than those of non-agile businesses. Achieving agility requires knowledge management and information exchange both inside the organization and with outside parties. An agile business adjusts its processes, routines, and resource configurations using knowledge of its internal and external environments. Although agility cannot be attained quickly, it should be included in the organization's long-term strategy (Ashrafi et al., 2006).

Organizational Agility enhances the swiftness and adaptability of significant business decisions, procedures, and issues (Heckler & Powell, 2016). Also, it has been shown that Organizational Agility can boost resilience, which is defined as an organization's capacity to recover from crises brought on by any internal, external, or environmental changes (Mrugalska & Ahmed, 2021). Managers across all sectors concur that Organizational Agility is a crucial success factor that defines a company's ability to compete in the uncertain business environment of today (Walter, 2021).

Organizational Agility is assessed based on a company's operational, partnering, and customer agility capabilities (Zaini & Masrek, 2013; Sambamurthy et al., 2003). An organization's customer agility is strengthened when its operational agility is vital because it can react more swiftly to client requests and shifting market conditions. Similar to how an organization with high operational agility can benefit from its partners' skills to increase its partnership agility, operational agility also benefits from having strong customer agility.

2.3.1 Operational Agility

An operationally agile company can rapidly and accurately spot excellent business prospects, eventually resulting in higher revenues and profitability (Zaini & Masrek, 2013). From previous research, an organization's capacity to handle information effectively and efficiently is crucial in establishing operational agility, particularly when recognizing and adapting to market changes (Huang et al., 2012). Another study discovered that using the knowledge gained from internal data and information analysis could assist firms in adjusting to and enhancing internal operations and processes (Ashrafi et al., 2006).

2.3.2 Partnering Agility

Partnering agility is the capacity of a business to work rapidly and productively with outside partners, such as vendors, distributors, and other stakeholders. It entails forging trusting connections, creating open lines of communication, and cooperating to accomplish shared objectives. It is also the capacity to coordinate partners, improve assets, and make use of expertise with partners (Ridwandono & Subriadi, 2019). To investigate the potential for innovation and competitive action, businesses might use partner agility to create a network of strategic, extended, or virtual partnerships (Sambamurthy et al., 2003).

2.3.3 Customer Agility

Sambamurthy et al. (2003) described customer agility as a company's capacity to use customer feedback to gather market knowledge and spot chances for competitive action. According to Ridwandono and Subriadi (2019), customer responsiveness is having the capacity to recognize user demands and satisfy them with goods or services. The idea of customer agility has also been linked to an organization's capacity for gathering and acting on customer-related market intelligence. If the organization does not act swiftly to satisfy the needs and expectations of its customers, the customers will turn to the goods and services provided by their rivals (Zaini & Masrek, 2013).

2.4 Relationship between Information Security Management and Organizational Agility

Agile organizations communicate information often, necessitating substantial safeguards for sensitive data (Dehaghi, 2016), so a cornerstone for agile organizations is Information Security. ISM is anticipated to support agility primarily by guaranteeing that all IT risks connected to organizations' information assets may be minimized and managed successfully. From previous studies, effective Information Security strategy implementation enhances organizational performance. Information systems security offers the foundation for detecting and acting upon opportunities with customers, partners, and suppliers, as well as internal processes to improve Organizational Agility, which improves overall organizational performance. ISMS, which provides centralized control and ensures access to accurate and timely information, is anticipated to boost Organizational Agility. ISM standards can significantly increase Organizational Agility by assuring data and information integrity, availability, and confidentiality for business purposes (Zaini et al., 2020).

2.5 Challenges related to Information Security Management

According to Hall et al. (2011), the unavailability of a proactive Information Security plan to make information visible, accessible, assured, and adequately safeguarded can cause disruptions in operations and pose significant dangers to the organization's performance and competitiveness of customers. Additionally, despite technological advancements that offer tools to defend information assets, more than technology is needed due to an increase in Information Security risks and vulnerabilities. From previous studies, it was realized that the management of Information Security is not only seen as a technological challenge but as much as a governance issue (von Solms & von Solms, 2004; Chang and Ho, 2006; Werlinger et al., 2008; Caralli, 2004). This emphasizes that business processes and organizational issues must be considered in addition to technical controls if the management of Information Security is to be successfully ensured (Choobineh et al., 2007).

Knapp et al. (2006), based on a survey carried out to identify and order the essential Information Security concerns for organizations, highlighted several issues with Information Security that firms worldwide face. This includes support from top management, policy-related problems, user awareness (training and education), access control and identity management, etc. According to them, regardless of an organization's size, industry, or location, the top concerns are often the same, with a few notable exceptions.

2.5.1 User awareness (training and education)

The human element is the most vital component of any security defense system, and employees must be adequately trained to identify and address issues (Purser, 2004). The understanding of Information Security and training directly impacts user compliance behavior. Lack of training leads to policy violations and the incidence of behavior that puts the organization at risk. End users' ignorance results in non-compliance, whereby they need to be made aware of the significance of Information Security and the associated organizational needs. A difference will be made if an organization has a thorough and effective Information Security culture and the users implement it (Alotaibi et al., 2016). Knapp et al. (2006) mentioned that a public awareness campaign promoting computer security should be launched with low-cost or financially supported training programs.

2.5.2 Top Management

Knapp et al. (2006) stated security is frequently only given lip service by management; it is not seen as a crucial aspect of corporate operations but rather as a cost and a burden. According to Ashenden (2008), a well-known communication gap exists between senior managers or board members and Information Security managers in an organization. Senior decision-makers have historically been challenging Information Security managers to persuade them of the necessity of Information Security since there is still a notion that Information Security is a technical subject and is best delegated and controlled by technical employees. Knapp et al. (2006) further advised that every firm and organization needs to create a top IT/Information Security post reporting directly to the CEO and establish clear legislative obligations holding upper management responsible for funding and supporting security.

2.5.3 Policy Development

The company's policy establishes broad guidelines and guarantees a unified approach to resolving typical problems. According to Choobineh et al. (2007), the "vehicle" for controlling the identified risks to the organization is Information Security and assurance policies. Even the best policies, practices, and procedures will only be effective if they are implemented. Many organizations need to update their policies to reflect technology's fast and continuously evolving nature. Organizations must regularly examine and update their policies to ensure that they still satisfy their needs and that any adjustments are communicated to all employees (Alotaibi et al., 2016).

2.5.4 Audit

Organizational ISM is thought to have Information Security Audit as a crucial component. An organization should therefore conduct internal and external Information Security Audits to ensure that its security policies, rules, and processes are followed (Singh and Gupta, 2013). Through the request of a third party's opinion, audits offer the chance to evaluate how well things function in actual practice. This helps prevent bias on a personal level (Purser, 2004). Irregular internal and external audit exercises on the policies and processes of Information Security in organizations could be seen as a challenge.

2.6 Summary

This chapter has highlighted the most frequent challenges associated with ISM. These factors include users' awareness, top management involvement, policy development, and audit. It also explained Organizational Agility as an organization's ability to recognize or impact environmental change and successfully respond to such change. This can be evaluated based on a company's operational, partnering, and customer agility skills. Overall, achieving organizational agility calls for a comprehensive strategy that considers every facet of the business and interpersonal interactions inside the organization.

3 Research Methodology

This chapter presents the choice of research methods including the research strategy, the data collection method, data sampling, data analysis methods as well as the research ethics.

3.1 Choice of Research Method

3.1.1 Research Strategy

According to Johannesson and Perjons (2014), a researcher must decide which research strategy to use among the many options available, which are survey, case study, experiments, phenomenology, ethnography, grounded theory, action research, and mixed methods, with their decision based on the objectives and specifics of the study they are doing. However, it is crucial that the technique chosen can be justified in terms of being feasible, ethical, and suitable for the right kinds of data to address the research topic, regardless of the option taken (Denscombe, 2010). Case study offers a detailed, in-depth account and insight into one specific occurrence of the studied topic (Johannesson & Perjons,2014). This allows for a thorough investigation and a deeper understanding of the topic. One major drawback of the case study approach is that it is most susceptible to criticism regarding the validity of the generalizations drawn from its findings (Denscombe, 2010). Not much generalization can be made can as it restricts how widely the findings can be applied.

Some alternative research strategies to a case study are surveys, phenomenology, and ethnography. Surveys are best used when a researcher looks for factual data on a specific group of people, such as their actions, thoughts, or personalities (Denscombe, 2010). According to Johannesson and Perjons (2014), one of the advantages of surveys is that they are most effective for gathering information on specific, well-defined topics. However, they are less effective for conducting in-depth research on complicated phenomena, making them less suitable for this research study. As explained by Latham (2016), phenomenology is centered on the participants' interpretations and feelings on their personal experiences. The participant's perspective is the primary consideration. It is interested in how individuals interpret and feel about certain concrete events. One of the downsides to phenomenology, as stated by Johannesson and Perjons (2014), is that it has been said that phenomenology lacks scientific rigor and is overly descriptive rather than analytical and explanatory, which is an essential requirement for this study.

Considering the different research strategies described the case study strategy due to its in-depth and deeper understanding of the topic best suits this research study and is more appropriate to address the research problem. Based on research carried out by Singh and Gupta (2019) on “Information Security Management Practices: Case Studies from India”, a case study research approach was used. Likewise, in a study “IT-enabled operational agility: An interdependencies perspective” conducted by Tan et al. (2017), it was stated that the use of the case technique is appropriate since we are looking for comprehensive responses to a series of exploratory and investigative "how" inquiries.

3.1.2 Data Collection Method

Denscombe (2010) mentioned that social researchers can use four main methods to collect data: questionnaires, interviews, documents, and observation. On the contrary, Johannesson and Perjons (2014) listed five of the most popular methods used in the collection of data as questionnaires, interviews, observation studies, focus groups, and document studies. For this research study, the primary data collection method that was used is the interview. Also, for the purpose of data triangulation, documents which is found on the website of the company was an alternative method in addition to the interview. This is in accordance with what was stated by O'Hair and Kreps (1990) that triangulation in research is the practice of combining a few distinct methodologies, measurement techniques, and data analysis procedures to confirm and boost trust in the findings of individual studies.

An interview is a conversation between a researcher and a respondent during which the researcher sets the agenda by questioning the respondent. The choice of the interview as the data collection method is that interviews are frequently used to elicit responses from respondents about their feelings, attitudes, opinions, and experiences (Johannesson & Perjons, 2014). This is the main essence of this study, to gather opinions from the respondents based on their experiences. The decision to go for a semistructured interview is that it gives room for the researcher to prepare questions before the interview but not limited to those questions. A little deviation is allowed. This made the semi-structured interview most suitable for this study as the questions were open-ended, allowing interviewees to bear their minds without restrictions to specific questions.

In addition to interviews, documents are another source of data. There are several types of documents, one of which is organizational records. They consist of meeting minutes, yearly reports, personnel files, sales data, and company notes. Comparatively to using interviews, using documents as a data source allows for the collection of a large amount of data more quickly and affordably. Documents have the drawback that it might be challenging to determine whether they are trustworthy (Johannesson & Perjons, 2014).

The Questionnaire is an alternate approach to gathering data for this study, and it is more effective when standardized data from identical questions is required. One of the drawbacks of questionnaires is the typical way questions are asked. The same set of questions is asked of all interviewees (Denscombe, 2014). This explains the rationale behind selecting a semi-structured interview as the data collection method, which permits freedom in how the questions are posed and answered.

3.1.3 Sampling Strategy

Samples could be representative or exploratory. Denscombe (2010) argues that the selection of samples can be made in two ways. Researchers can employ either non-probability or probability sampling to select their sample from the research population. While probability sampling is effective in large-scale studies using quantitative data, non-probability sampling is influential in small-scale studies using qualitative data. When researchers find it challenging or unpleasant to choose their sample based solely on chance, they adopt non-probability approaches to sampling, which do not work on the premise of a random selection of the sample. On the other hand, in order to generate an exploratory sample, purposive sampling is a helpful strategy that aids in identifying a small group of people who can supply very relevant information to the researcher (Johannesson & Perjons, 2014).

For this study, which is small-scale research, an exploratory sample was used, while non-probability sampling using qualitative data and purposive sampling methods was used to select the participants. These was based solely on the experience and expertise of the participants. Since the research is on the management of Information Security in organizations, the research population is information security experts in an organization. However, it was not feasible for the researcher to reach out to all security specialists. Sampling was done such that few security experts were selected from a particular organization to participate that will help provide relevant information for the study as not all employees of the organization are security experts. Regarding the selection of appropriate sample size, Marshall (2013) mentioned that the classification of case studies is one of the most challenging aspects of qualitative research. Yin (2009) also "recommends at least six sources of evidence for a single case study" (p.13). Having the right sample size and the quality of data received from the participants will help achieve data saturation. The concept of data saturation according to Francis et al. (2010) is crucial because it considers whether a theory-based interview study is likely to have obtained a sufficient sample for content validity.

An alternative approach to getting sample methods is the representative sample using quantitative data. According to Denscombe (2014), the aim of getting a representative sample is when the numbers involved tend to be relatively large. In addition, an alternative approach to selecting samples is probability sampling which is used for large-scale surveys for a representative sample, whereas this research study is small-scale. Therefore, probability sampling is not the best fit for this study because choosing samples is only reliant on chance, which researchers find problematic, hence the reason for choosing non-probability sampling.

3.1.4 Data Analysis Method

According to Braun and Clarke (2006), the thematic analysis should be considered a core method for qualitative analysis because qualitative methodologies are immensely diverse, intricate, and nuanced. *Thematic analysis* is a versatile and practical research approach that may produce a complicated, rich, and detailed description of data. It is a method for identifying, analyzing, and enumerating patterns in data.

Due to the data collection method that was used for this study which is semi-structured interviews, the outlines provided by Braun and Clarke (2006) will serve as a guide wherein the data will be analyzed in six stages. These are:
Phase 1. Familiarizing with the data: It is essential that one becomes fully acquainted with the depth and breadth of the information by immersing oneself in it. This can be achieved by transcribing the data that will be obtained from the interview into a written format.
Phase 2. Generating Initial Codes: This phase begins after the data has been reviewed by the researcher and has come up with a preliminary list of ideas on what is in the data and what makes it interesting. The creation of preliminary codes from the data follows in this phase.
Phase 3. Searching for themes entails grouping the various codes into potential themes and assembling all the pertinent coded data extracts within the discovered themes.
Phase 4. Reviewing themes: After a list of potential themes has been created, it involves refining those themes.
Phase 5. Defining and naming themes: This is the phase where the themes that will be provided for analysis will be specified and improved upon, after which the data within them will be analyzed. **Phase 6.** Producing the report: This phase begins when one has a set of fully developed themes and involves writing the report's final analysis and conclusion.

Asides from the thematic analysis, there are different approaches to analyzing qualitative data. According to Denscombe (2010), for content analysis, concentrating on specific instances of words taken from the text poses no issue, also, there is a heavy emphasis on measurement, and it is noteworthy because even though it is combined with qualitative data, it still yields quantitative measurements. Thematic analysis was chosen for this study as it is the widely used method of analysis for qualitative research by researchers.

3.2 Application of Method

3.2.1 Application of the Case Study

The case study was carried out in one of the financial institutions in Nigeria. The company has requested to remain anonymous, and their wish was respected. For the sake of this study, the company will be called Company “XYZ”. In line with the information gotten from the organization’s website, Company “XYZ” is one of the top commercial banks in Nigeria with a solid track record in trade financing, risk management, and compliance. To remain relevant in the industry while maintaining its record, Company

“XYZ” places much value on the security of its assets and information systems and compliance with industry-wide rules and regulations. The company has existed for more than 20 years with several branches, and the extension of its operations to subsidiaries all across the globe. Customers can place their money in the care of this institution based on the level of trust built over the years. These would not have been achievable without an effective ISM. Hence, the reason for reaching out to one of the security specialists in the organization was to discuss how the company has been able to maintain its integrity, security-wise, over the years and how it has been able to manage ISM to control risks while maintaining organizational agility.

3.2.2 Data Collection Method

A semi-structured interview was the data collection method used for this study. Using the purposive sampling technique, based on the existing relationship between the researcher and the organization and the top-notch services received over the years, the researcher believed the selection of participants from this organization would most likely yield the most valuable data. This spurred the researcher to email the company's Head of the Threat Intelligence and Incident Response team, explaining the nature of the study. He was pleased to grant the researcher's request. He willingly suggested and helped motivate other security experts in his group. Before the interview sessions, the participants were briefed on the aim and nature of the study, after which they chose convenient dates to conduct the sessions. The researcher also developed interview questions (as shown in Appendix B) related to the research topic, which served as a guide during the interviews. However, the questions were open-ended as the participants were allowed to bare their minds without being restricted to the set questions, bearing in mind that the overall aim of the interview sessions was to answer the study's research question. This was achieved via Zoom calls, where the sessions were recorded and transcribed afterward. Based on the alternative data collection method, which is documents, the researcher also carried out an analysis of the company's documents as uploaded on their website in other to have a better understanding of how the organization operates, the vision, mission, core values, products offered, and many others.

Initially, five interviews were conducted where adequate diverse views were gathered. Afterward, two more interviews were conducted to investigate if any new themes would emerge outside of those already gotten from the initial five interviews. However, no new themes were generated for the last two interviews indicating the point of data saturation, which made a total of seven participants. The researcher believed seven participants were sufficient to gather enough data to comprehend the phenomenon being examined adequately. Data triangulation was achieved based on the knowledge gained from the interview sessions coupled with the information obtained from the company's document as uploaded on their website.

Table 1 presents the positions of the selected participants.

Participant	**Role of the Participant**	**Years worked in the Organization**	**Date of Interview**	**Duration (in minutes)**
1	Team Lead: Security Policy, Governance, and Compliance	5	18-03-2023	36
2	Head: Threat Intelligence and Incident Response	7	21-03-2023	50
3	Analyst: Threat Intelligence and Incident Response	2	22-03-2023	36
4	Unit Head: Security Technology and Engineering	3	25-03-2023	52
5	Analyst: Threat Intelligence and Incident Response	3	28-03-2023	39

6	Analyst: Threat Intelligence and Incident Response	2	30-03-2023	54
7	Analyst: Vulnerability assessment and Penetration testing	5	01-04-2023	43

Table 1 Participants Information

3.2.3 Data Analysis Method

The data analysis method was according to the six steps of the Thematic analysis which are: familiarizing with the data, generating initial codes, searching for themes, reviewing themes, defining and naming themes and producing the report. After the interviews were conducted through recorded audio zoom sessions, the recordings were later transcribed with the help of a transcribe app and manually in situations where clarity was needed by repeatedly listening to the recordings to ensure adequate information was obtained. This is in accordance with what was said by Braun and Clarke (2006) that if your data has already been or will be transcribed for you, it is essential that you spend additional time familiarizing yourself with the details and verifying the accuracy of the transcripts against the original audio recordings. The data obtained from the transcription were analyzed using inductive reasoning which includes finding codes and patterns in the data, then making judgments based on those patterns. Also, the documents were read and interpreted to identify themes and patterns. These codes are then categorized into themes and sub-themes.

Table 2 as shown below presents an example of how the initial codes, theme and sub-themes were generated using an inductive reasoning.

Snippets from Interviews	Codes	Sub-Themes	Themes
” ...When we need to carry out training for all staff, once it's coming from the top, we understand that management is aware of this, and then they take it more seriously [...] especially when you want to carry out awareness and training, you just must make sure the executive management is aware of their stake. And once you do that, you have their full support...” ***Participant 1***	Routine training, Communication, Support	Effective Communication, Management Involvement	Management support

Table 2: Thematic Analysis Illustration

3.3 Research Ethics

According to Denscombe (2010), social researchers are required to approach their work with ethics. This assumption is morally justified by the idea that the public needs to be shielded from academics who could be tempted to employ any means necessary to increase knowledge regarding a particular topic. Furthermore, Denscombe (2010) stated the four principles of research ethics (a) protect participants' interests, (b) guarantee that participation is voluntary and founded on informed consent, (c) prevent deceit and uphold scientific integrity, (d) complies with local and international regulations.

Thus, for this study, all the principles will be satisfied. In lieu of this, the participants' interests and anonymity will be safeguarded by guaranteeing the confidentiality of the provided information. Also, as shown in the consent form (Appendix A), where it is clearly stated that participation is voluntary, the participants will be briefed about the nature of the study and their consent will be secured prior to conducting the interviews. Thirdly, an overview of the research's objectives will be presented to the participants to avoid deception or making false statements. Lastly, to comply with laws and regulations, the data collected would be protected and kept confidential which will help fulfill and adhere to the legislation governing copyright and intellectual property issues.

4 Results

This chapter introduces the results of the data analyzed with a breakdown of the themes and sub-themes as identified.

This study has been able to point out measures in which organizations manage Information Security while maintaining agility with Company "XYZ" as the case study. With the data that was collected from the organization, the thematic analysis done revealed eighteen measures which are the sub-themes, and these were further categorized into eight themes.

The figure below presents the themes and sub-themes as identified. The themes are colored in green while the sub-themes are colored in yellow.

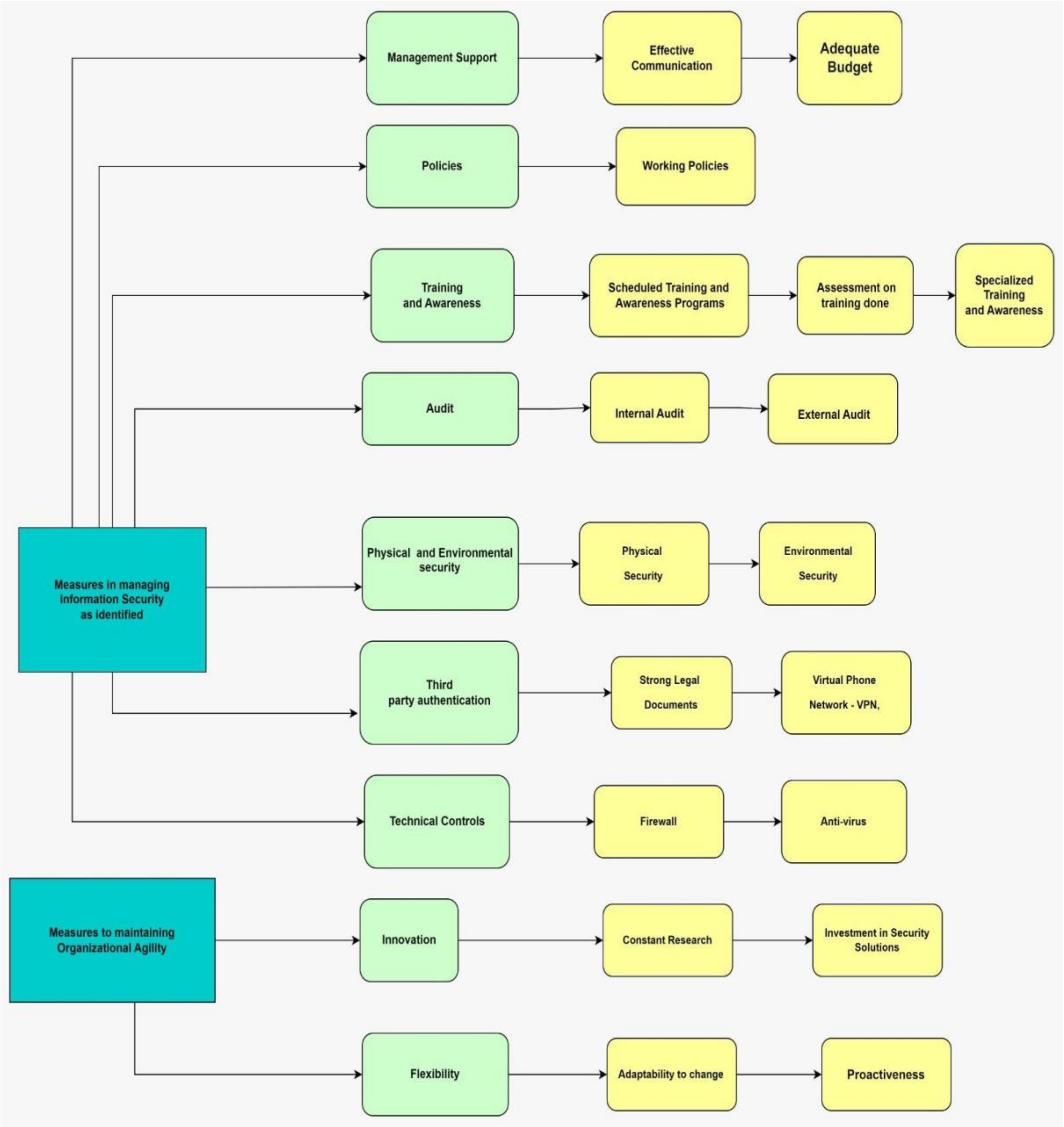
Measures in managing Information Security as identified
Management Support
Effective Communication
Adequate Budget
Policies
Working Policies
Training and Awareness
Scheduled Training and Awareness Programs
Assessment on training done
Specialized Training and Awareness
Audit
Internal Audit
External Audit
Physical and Environmental security
Physical Security
Environmental Security
Third party authentication
Strong Legal Documents
Virtual Phone Network - VPN,
Technical Controls
Firewall
Anti-virus
Measures to maintaining Organizational Agility
Innovation
Constant Research
Investment in Security Solutions
Flexibility
Adaptability to change
Proactiveness

Figure 1 Thematic Analysis with themes and sub-themes

4.1 Management Support

The result of these findings indicates that management support is one of the essential components of effective information security management and organizational agility. The analysis also revealed that effective communication and adequate budget play essential roles in maintaining acceptable information security practices at the case company.

4.1.1 Effective Communication

Effective communication is the exchange of knowledge, information, opinions, and data to ensure that messages are received and comprehended with purpose and clarity. Some of the participants spoke on the impact effective communication with the top management has had on the successful management of the organization's Information Security. One of the participants mentioned that due to the IT savviness of the executive management, communication is smooth, the security managers do not have to spend so much time explaining their requests before it is understood and accepted. Another participant explained that due to the level of support received from the management in recent times, it has made communicating with them a lot easier.

Another participant also mentioned the importance of having effective communication with the management which helps the team a lot in delivering well on their job functions. For example, due to the relationship that the Information Security group has built with the management over the years that makes communicating with them much easier, the team has been able to get management involved when some information or training relating to information security need to be passed across to the staff. This leads to receiving fast response from the staff members.

4.1.2 Adequate Budget

This has to do with having sufficient finance earmarked to support Information Security activities. Few of the participants stated that due to the recent happenings in the cyber security space, the executive management has made it a priority to invest in security solutions as well as the people to better manage its Information Security and Organizational Agility. One of the participants also commended the management on its recent involvement and buy-in when it comes to security solutions and resources.

One of the participants however suggested that the management can still do better when it comes to budgeting for security solutions. She added that top management need to go beyond seeing Information Security as mere cost center and not only looking at its cost implication while at times give priority to the security of the bank by providing more financial resources.

4.2 Policies

Another measure as revealed by the analysis is Information Security policies which provide a precise and consistent framework for protecting priceless information assets and guaranteeing adherence to relevant laws and regulations. Having the policies working as expected will go a long way in successfully managing Information Security in an organization.

4.2.1 Working Policies

An organization's policies must be properly executed and enforced to be said to have working policies. All the participants agreed that the organization has sufficient and working policies in place which makes the management of Information Security a lot easier. They further spoke on the effectiveness and the frequency of review of the policies which helps the organization to drive compliance. They stated that many of the policies are at least reviewed annually or on a need basis when it is necessary.

The need for adherence to these policies as highlighted by one of the participants is to get certified and avoid the consequences of non-adherence, follow through with the frameworks and guidelines already set and avoid being sanctioned.

However, some of the participants pointed out the areas in which the organization could do better pertaining to policies. One of them revealed that more work is needed in getting staff and vendors to adhere to some of the policies in the organization. Another area of improvement, as highlighted by another participant, is regarding accountability from all the business units. She explained that each unit should be able to embrace the policies that concern them and have them well documented.

4.3 Training and Awareness

Training and Awareness refer to the process of informing stakeholders, including employees, on the information security policies, processes, and best practices used by the firm. As revealed from the analysis done, creating scheduled and specialized training and awareness programs, and conducting assessments after the training has been done are the three sub-themes.

4.3.1 Scheduled Training and Awareness Programs

These are structured training programs such as online courses, training in the classrooms, etc. All the participants spoke on the level of training and awareness organized by the company, the schedules in which these are carried out, and the impact/benefits achieved just to ensure the Information Security of the organization is well managed. According to one of the participants, it was explained that there are schedules in place for training and awareness, such as creating fliers and banners and sending them to all staff to keep them informed. Another participant corroborated by saying that this training mostly happens on a quarterly basis just to ensure that staff members do not forget what is expected of them when it comes to security matters. He also added that awareness is carried out on a frequent basis.

> *We have a schedule, […] we create like fliers, a banner on basic training, clear screen and send it out to all staff. We also have proper training sessions that could be on virtual channels. Other times, we also engage in physical training, where we get facilitators to talk on a specific security topic. We also sometimes enroll Users on the security training platform, where they undergo self-paced training with an assessment at the end. So, we devise several ways of training* (Participant 1)

4.3.2 Assessment of Training Done

This speaks on how the organization conducts assessments/tests for the employees after each training to test their level of understanding and a certification of completion is presented to successful staff. One of the participants explained that the organization does not only stop at training its staff, but it also takes a further step to test their knowledge of what they are being trained on to be sure the staff have been adequately trained to prevent having weak links that could expose the organization to threats.

4.3.3 Specialized Training and Awareness

Asides from the general training and awareness conducted for all staff of the organization, it is equally important to have training and awareness targeted to specific departments or job roles. Two of the participants spoke on the need for role-based training, giving the appropriate training to the right audience.

In addition, the participants gave good remarks on the benefits of the regular training and awareness conducted as seen on the part of the staff. Another participant also mentioned the positive impact of this training and awareness, as seen in the response of the staff to suspicious and phishing emails.

4.4 Audit

As indicated from the results of this study, an audit is a significant component of organizational ISM. The processes, systems, and controls of a company are objectively evaluated via audits, which can help to identify problem areas and reduce risks. The analysis further revealed that Internal and External Audits play crucial roles in managing Information Security and Organizational Agility.

4.4.1 Internal Audit

Internal audit's primary goal as explained by the participants, is to give management and other stakeholders of the organization independent, unbiased assurance that the company operates in compliance with internal policies, laws, and regulations and that its assets are protected from fraud. They further explained that in certain instances, the internal audit needs to be carried out before engaging in the external one. It was added that engaging in the internal one helps to prepare the organization ahead of the external one for validation.

The participant also mentioned the areas that needed improvement when it comes to carrying out internal audits in the company. She explained that much effort is not put into internal audit as opposed to the external one and feels if the internal audit is taken more seriously, it will be of much benefit to the organization.

4.4.2 External Audit

The participants admitted that it is not sufficient to only conduct internal audits. It is still necessary to complete the external audit by giving room to an external party to evaluate the organization's security policies and processes. It was revealed by one of the participants that engaging in external audits coupled with the internal one gives the company some level of confidence and assurance. Another participant mentioned that an added criterion to the external audit is the certification that is awarded to the company when all the criteria is met such as PCI DSS and ISO standards.

4.5 Physical and Environmental Security

Physical and environmental security is yet another measure indicated in the findings of this study. It helps the organization reduce the dangers of physical and environmental risks to their vital assets and operations.

4.5.1 Physical Security

According to the participants, physical security in an organization has to do with the protection of its physical assets, most importantly its data center. The data center of an organization must be guarded heavily because an intrusion into this space can lead to a compromise in the security of its data and valuable information. Some of the participants mentioned the measures in place to ensure physical security is maintained in the organization. This includes the presence of security men in strategic locations, CCTVs, biometrics, registers, etc.

4.5.2 Environmental Security

On the other hand, environmental security as explained by one of the participants refers to the measures taken to protect a building or infrastructure such as the data center against dangers that could interfere with its normal operation. This is equally as important as the physical security of the data center. He explained that the organization has the HVAC - Heating, Ventilation, and Air Conditioning system in place to prevent fire, overheating, etc. of the organization's assets.

4.6 Third Party Authentication

Another equally important measure that aids the successful management of Information Security as identified from the findings of the study is third party authentication. The analysis revealed two subthemes, Strong Legal Documents and Virtual Phone Network -VPN.

4.6.1 Strong Legal Documents

Integration with third parties has become a common practice recently, and the participants admitted that measures such as written agreements stating the roles and responsibilities between both parties are put in place by the organization to ensure valid authentication before a successful connection can be granted to these external parties in other to prevent the undue exposure of the bank to external forces. One of the participants also explained the need for the organization to integrate with these external vendors, which are mainly for revenue generation.

4.6.2 Virtual Phone Network – VPN

The VPN is another measure put in place for third-party authentication, as revealed by the participants. A few of the participants further explained how the VPN works by creating a secure connection between the VPN server and the user's device, thereby causing the traffic that passes through the tunnel to be encrypted, protecting it from third-party eavesdropping, interception, and tampering.

> *What we have in existence is the VPN – Virtual Private Network. It creates a secured tunnel they are to communicate with the bank and reach our resources without attackers or people eavesdropping into their communication with the bank, so the VPN takes care of that (Participant 6)*

4.7 Technical Controls

Technical Control is another identified measure from the findings of this study. It uses certain security technologies and mechanisms to enforce security policies, processes, and standards making the management of Information Security and Organizational Agility a lot easier. Some of the aspects further revealed from the analysis are Firewall and Anti-virus.

4.7.1 Firewall

Based on the conversations with the participants, a firewall helps to monitor and manage incoming and outgoing network traffic to guard against unauthorized access, denial-of-service attacks, and other network-based security risks.

4.7.2 Antivirus

This is another control mentioned by the participants that helps to protect the organizations assets against breaches and intrusion. The participants confirmed the efficacy of the anti-virus systems in place in the organization. Another participant also added that the anti-virus systems in place within the organization are strong enough to detect and catch any bug in the system.

4.8 Innovation

One of the key drivers of Organizational Agility, as identified from the findings of this study, is Innovation. It helps organizations remain ahead of the curve and quickly adjust to changing circumstances in a corporate environment that is undergoing rapid change. Due to further analysis, two aspects, Constant Research, and Investment in Security Solutions, were revealed that help the organization to be innovative and agile while at it.

4.8.2 Constant Research

This speaks to how the organization keeps looking for new ways to meet customers' needs, identify opportunities in the market space to stay ahead of its competition. One of the participants revealed that the organization keeps making use of different tools to carry out research and how they can be a step ahead of hackers and attackers.

> *[...] From time to time we are constantly doing our research. I mean using open-source tools and some proprietary tools to get a lot of intel on threats and attackers on their techniques and all of that* (Participant 3)

4.8.3 Investment in Security Solutions

For an organization to be agile and continuously protect its Information Security, it must be willing to invest in security solutions and its people to help them come up with better and innovative ways of protecting its asset. This could be in the form of management earmarking adequate budget for training, seminars and awareness for its research and development security team or foreseeing into the future and acquiring necessary solutions that will help protect the organization's asset and information from being compromised. According to one of the participants, it was revealed that management is always willing to carry out assessment of security solutions proposed with the decision to invest based on the outcome of the assessment. Another participant added that the organization has a huge budget for training its employees and creating awareness since humans can be one of the weakest links through which an organization can be invaded by attackers.

4.9 Flexibility

Another important characteristic of an agile organization, as revealed in the findings of this study, is Flexibility which refers to the capacity to adjust to evolving situations or events. Two basic aspects discovered from the analysis are Adaptability to Change and Proactiveness.

4.9.1 Adaptability to Change

Because of the vulnerability of the data and information that is being processed and transmitted by the case study organization being a financial institution, one of the participants explained why it is important for the organization being agile to move as things change. She further stated that the attackers are looking for new ways to strike at the bank, and so the organization must be willing to always adapt to these changes and come up with new ways to protect the organization. It was also revealed by another participant that with the evolvement of FinTech companies, the organization has been able to change from its traditional method of action to accommodate and communicate easily with the FinTech companies.

4.9.2 Proactiveness

Being proactive is having the capacity to foresee and prepare for potential future occurrences, issues, or opportunities. One of the participants spoke on how the organization has been proactive when it comes to satisfying its customers and offering new solutions.

> [...] *For instance, in my country, like some weeks back we had this cash crunch and customers needed to go fully digital. One thing the organization put in place is proactiveness. The organization has been looking for payment methods that will serve the customers better, such that the organization is integrated into the customers' everyday lives by being able to make payments seamlessly. When there was that cash crunch, all we needed to do was to probably include the features that were already being worked on to make the organization's mobile applications more accessible and faster* (Participant 5)

However, some of the participants also suggested the measures the organization can take to be more agile which includes having fewer rigid structures, embrace diversity, and automation of processes as much as possible.

5 Discussion

This chapter presents the discussion of the study comparing how company "XYZ" has been able to manage ISM while maintaining agility with those identified from previous research.

As revealed by the participants, the organization has so far achieved success in managing its Information Security, not as a stand-alone entity but with the inclusion of agility. It was also explained that the management has come to understand that for the organization to stay ahead of its competitors regarding the security of its information and asset and not give room for attackers to invade, it must be flexible. As technology is evolving and attackers are also looking for new ways to strike, the organization must be proactive enough to develop new security solutions that will better help protect its information and be willing to adapt to change. The participants spoke about how the organization is always quick to accept and adapt to changes which has helped it to remain relevant and competitive. This is because the attackers develop new attack methods and techniques so quickly to attack the organization's assets and data, which has spurred the organization to quickly change from its current countermeasure strategies and develop new ones to act against these attacks.

It was further explained that in other to adapt to market changes; the organization can handle information effectively and efficiently, thereby establishing operational agility. Also, regarding partnering agility, in a bid to better manage its Information Security, the organization has recently improved its capacity to work rapidly and productively with outside partners, such as vendors and Fintech companies. Lastly, it was mentioned that in other for the organization to suit customers' needs and regularly protect their information, it takes their feedback more seriously and continuously looks for new ways to satisfy them better thereby achieving customer agility.

5.1 Management Support

The flexibility and level of support received from the executive management of an organization make it a lot easier to successfully manage Information Security. As suggested by Ashenden (2008), it was stated that one of the ways to address the challenges associated with the management of Information Security is through effective communication with senior managers and end-users. Many of the participants revealed that efficient communication with the management of the organization has had a good impact on the management of its Information Security. Communicating with them or needing their permission and buy-in is not much of a tedious task based on their flexibility and intentional support of the group in anything relating to information security.

Furthermore, from previous research, Knapp et al. (2006) advised that every organization must set up a senior IT position reporting directly to the CEO and implement laws that clearly hold higher management accountable for funding and supporting security. This is in line with what was explained by some of the participants that the management has been more supportive when it comes to being proactive to invest in security solutions due to the recent happenings in cyber security space and is more willing to allocate resources to help protect the asset, data, and information of the organization.

One major challenge which needed to be improved on, as mentioned by one of the participants, is how management sometimes sees Information Security as a cost or a burden rather than seeing the value being added. This is in line with what was said by Knapp et al. (2006) that management views security as a cost and a burden rather than as a necessary component of organizational operations. However, some of the participants also suggested the measures the organization can take to be more agile, which include having fewer rigid structures, embracing diversity, and automation of processes as much as possible.

5.2 Policies

In addition to having appropriate and effective policies in place, it is crucial for an organization to make sure that the policies are regularly evaluated when due or on a need basis by willing to adjust to changes when new policies are made. It is equally essential that the policies are adhered to, to avoid being exposed to threats and sanctions. According to De Lange et al. (2016), policies strive to regulate information security, and they function similarly to organizational laws. One of the participants highlighted the necessity of adhering to these policies to be certified and prevent the negative effects of non-adherence. All the participants attested that the policies in the organization are regularly reviewed for effectiveness. According to previous research by Alotaibi et al. (2016), organizations must frequently review and revise their policies to make sure they continue to meet their needs and that any changes are communicated to all employees.

However, some areas where the organization could do better when it comes to policies, as mentioned by some of the participants, are management enforcing staff to adhere to these policies, and each business unit being held accountable to policies relating to their units.

5.3 Training and Awareness

It was stated by Purser (2004), from previous research that any security defense system's most crucial aspect is its human component, so staff members need to receive proper training to recognize and address problems. The participants spoke on how the organization through the Information Security team proactively organize scheduled training and awareness programs to train and constantly create awareness to remind the employees of the dos and don’ts of Information Security and to keep them regularly updated. Some also revealed that there are usually assessments conducted based on the training and awareness done to test the understanding of the employees and get to know the areas that still need to be emphasized. In addition, two other participants mentioned that asides the generalized training, there are also role-based training that employees engage in with focus on the areas that speak to their job functions.

Furthermore, all the participants spoke on the positive impact the training and awareness have had on the employees of the organization. It was stated that there have been lesser clicks on phishing emails which would have exposed the bank to threats, and less frequent sanctions since there are now fewer offenders. This is in line with what was explained in a previous study by Alotaibi et al. (2016) that if an organization has a thorough and successful Information Security culture and the users adopt it, a difference will be created.

5.4 Audit

Audits, according to Singh and Gupta (2013), are important instruments for evaluating an organization's implementation of information security and its adherence to regulatory standards. The audit is basically broken into Internal and External, as stated by the participants, which are in line with what was also stated by Singh and Gupta (2013) from previous research that a company should carry out both internal and external Information Security audits to make sure that its security guidelines, procedures, and policies are followed which is a crucial component for organizational ISM. Internal audit, as revealed by some of the participants, is when the organization is agile and proactive enough to prepare and carry out some checks in relation to its stance and adherence to policies and guidelines prior to when an external audit takes place. Furthermore, the participants mentioned that external audit is mostly carried out by independent third parties to evaluate and validate the organization's security policies and processes and to see if the organization complies with industry and global standards, thereby getting certified.

However, some of the participants suggested that much importance should be given to Internal audits as is given to External which will be beneficial to the organization.

5.5 Physical and Environmental Security

It was explained by Ma et al. (2008) from a previous study that physical and environmental security helps to guard against unwanted access, harm, and interference with corporate facilities and data. The participants applauded the level of security assigned to the organization's data center. They mentioned that the organization is agile in this regard, regularly willing to adapt to new ways that will help better secure the data center ranging from the presence of security men to CCTVs, biometrics, presence of registers for signing in and out, amongst many others. All these have helped the organization to heavily protect its physical assets against attackers. This is supported by Zaini et al. (2020) from previous research where it was mentioned that by safeguarding an organization's physical environment, you could make sure that sensitive and important data, as well as information processing facilities, are safe from external threats and intrusions.

In addition, Environmental Security, as explained by one of the participants, refers to the environmental regulations in place, such as the HVAC - Heating, Ventilation, and Air Conditioning system that helps to protect the organization's critical infrastructure, such as the data center, against threats that could interfere with its regular operation. According to Zaini et al. (2020), as stated in previous literature, security precautions are essential for preventing espionage, theft, and damage from accidents, fires, and natural disasters, as well as protecting computers, related equipment, and their contents.

5.6 Third Party Authentication

This is a type of system access control with new measures on how the organization manages its Information Security. Some of the participants spoke on the importance of partnering agility which is the organization integrating with third parties. This is another source of revenue generation necessitating the need to have written agreements in the form of legal documents to draw out the roles and responsibilities of both parties and the consequences of not sticking to the agreement. The participants further revealed how the organization has been able to use *Virtual Phone Network – VPN* successfully to achieve third-party connectivity using secured tunnels to prevent attackers from eavesdropping on the communication between both parties.

5.7 Technical Controls

Technical controls, according to Zaini et al. (2020), typically consist of products and procedures (such as firewalls, antivirus software, intrusion detection, network controls, backup capabilities, and encryption techniques) and are primarily focused on safeguarding an organization's IT assets and the data that is transmitted over and stored in those assets. Some of the participants highlighted that Firewall is one of the safeguards the organization has put in place to guarantee that only legitimate connections that are authorized are permitted to enter and exit the organization's network. Other participants stated that Antivirus software is usually installed on all endpoints, such as servers and user workstations, and the organization is quick enough to purchase the updated version to protect against breaches and intrusion into the organization. This is backed up by Ma et al. (2008), that all systems should be secured with antivirus or firewall software.

6 Conclusion

This chapter presents the study's conclusion, limitations and future research, the originality and significance of the study as well as its research quality.

Information Security is very crucial in organizations as it seeks to safeguard the availability, confidentiality, and integrity of their information. Therefore, it is necessary to manage the organization's Information Security and be agile while at it as new trends of threats and attacks are being discovered. Therefore, the aim of this research is to investigate the management of Information Security in organizations while maintaining organizational agility and highlight the challenges encountered; the research question to be answered is *"How do organizations manage information security while maintaining organizational agility?"*.

The study's findings can help firms improve their information security measures by pointing them toward appropriate practices and solutions. Thus, personal and financial information, as well as other sensitive data about individuals are further protected. Also, by learning how to strike a balance between information security and organizational agility, businesses should put preventative measures in place to reduce cyber dangers. This can involve building incident response plans, regularly conducting risk assessments, and adopting strong security policies. This will help increase both personal and corporate safety and protection in the society with fewer cyber threats. Likewise, businesses may build solid relationships of trust with their clients, partners, and stakeholders by managing information security while preserving organizational agility.

By addressing ethical consequences, the study can highlight the significance of corporate transparency, which includes transparent privacy rules, data breach notifications, and effective dialogue with stakeholders about security procedures. The study can also encourage the responsible use of data by ensuring that businesses only gather and utilize data legitimately and in a way that upholds individual liberties and cultural norms.

Overall, the study on managing information security while maintaining organizational agility contributes to a safer and more resilient society where people can engage with digital systems with confidence, having the assurance that their data and information is secure.

6.1 Limitations and Future Research

Having carried out this research with only seven participants from one financial institution is on its own a limitation. As the research title is on managing Information Security in organizations, the opinion, and expressions of the participants from one organization in Nigeria do not automatically apply to other organizations. The measures Company "XYZ" applies to manage its Information Security might not apply to other industries and there could be other measures in which other organizations manage theirs not mentioned.

Another limitation was the unstable internet connection with some little glitches since the interviews were conducted online and not face-to-face due to the distance barrier. This made the transcription a bit incoherent in some cases resulting in the researcher having to spend more time doing manual transcription.

As a result of the limitations mentioned above, the researcher suggests that in the case of future research, more time should be allotted to the research study to allow for a comprehensive study to be carried out across different industries in other to gather diverse opinions and compare results. Also, in the absence of time constraints, the interviews can be conducted face-to-face so the researchers can meet with the participants and be able to study their behaviors and attitudes while conducting the interviews.

6.2 Originality and Significance

6.2.1 Implication for Theory and Practice

For the theoretical aspect, the measures as identified in Company “XYZ” has some similarities with those already mentioned in previous studies. This shows that the ways in which Information Security is managed across various organizations bear some correlations. However, with the newly identified measures, this could serve as a contribution and addition for other companies to use to better manage their Information Security. On the practical aspect, from the findings, some of the measures of managing Information Security categorized under this theme, third-party authentication, could be seen as challenging. This is because with the evolvement of FinTech, organizations must keep making connections to these FinTech companies to make revenue and stay relevant and by so doing increase their exposure level because of eavesdropping from attackers and the like. Hackers and attackers keep looking for new ways to attack, so these organizations also need to be agile and proactively search for safer ways to safeguard their assets and information, so they are not outsmarted. Moreover, these findings can also help organizations improve their connectivity to external parties and have various safeguards in place to protect their assets.

6.3 Ethical and societal consequences

The conduct of this investigation considered moral ethical and societal implications. According to the study's findings, there might be some positive ethical considerations such as prioritizing the protection of individuals’ privacy rights. The organizations can develop privacy safeguards that ensure that personal information is handled with the utmost care, thereby lowering the danger of misuse or unauthorized access, such as secure data transmission and storage, data collecting based on individual consent, and well-secured data collection. Additionally, organizations can be urged to be open and honest about how they handle customer information and data, ensuring that they do not stray from the stated purpose for which it is being collected.

Regarding the societal consequences, information security as well is its management is key in organizations. Hence, this study will further help the management and security experts in the organization on how they can better manage information security and being agile while at it. Furthermore, it can also be of much benefit to other organizations most especially financial institutions due to their similar characteristics such as regulatory frameworks, organizational structures, market conditions to effectively secure their information. Overall, this study makes society safer and more robust so that people may interact with digital systems with confidence knowing that their data and information is safe and secure.

6.4 Research Quality

To assess the reliability of qualitative research, the criteria frequently utilized, according to Stenfors et al. (2020), are credibility, transferability, confirmability, and dependability.

Credibility: This requires that the methods used be well justified and explained. To maintain credibility in this study, the researcher opted for semi-structured interviews as the data collection method alongside getting information from documents on the company's website which allowed for fewer in-depth interviews that offered deep information in comparison with the information gathered from the website. This made the study's findings believable and reputable and in accordance with data triangulation.

Transferability: This refers to how results may be applied to a different setting or group beyond the particular study sample. "Settings" is used here to describe the specific social, physical, or organizational context (environment) that the findings may be implemented in. To ensure transferability is achieved, the case study is focused on a financial institution in Nigeria, and to some extent, the study's findings may be applied to other financial institutions in the same setting that share similar characteristics such as regulatory frameworks, organizational structures, market conditions, etc since their mode of operations is somewhat similar.

Confirmability: To maintain confirmability, the researcher kept an open mind coupled with the fact that semi–structured interview was the primary data collection method which gave room for the participants to express their opinions without the researcher forcing them or being rigid. The evidence derived from the interviews was also in synchronization with the conclusions made at the end of the study.

Dependability: Based on the credibility and reputation that was built, the study could be repeated under comparable circumstances to a large extent. The research has been clearly written out. Also, the interview questions were provided with motivations for the purpose of clarity. This makes it easy and comprehensible enough for other researchers to make use of.

References

Alotaibi, M., Furnell, S., & Clarke, N. (2016). Information Security Policies: A Review of Challenges and Influencing Factors. In the 11th International Conference for Internet Technology and Secured Transactions (ICITST-2016), (352 -358).

Ashenden, D. (2008). Information Security management: A human challenge? Information security technical report, 13, 195 – 201.

Ashrafi, N., Xu, P., Kuilboer, J. P., & Koehler, W. (2006). Boosting Enterprise Agility via IT Knowledge Management Capabilities. Proceedings of the 39th Hawaii International Conference on System Sciences – 2006.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology, 3 (2)*, 77-101. http://dx.doi.org/10.1191/1478088706qp063oa.

Caralli, R. A. (2004). Managing for Enterprise Security. CarnegieMellon Software Engineering Institute, CMU/SEI-2004-TN-046.

Chang, E. C., & Ho, C. B. (2006). Organizational factors to the effectiveness of implementing information security management. *Industrial Management & Data Systems, 106(3)*, 345–361.

Choobineh, J., Dhillon, G., Grimaila, M. R., & Rees, J. (2007). Management of Information Security: Challenges and Research Directions. *Communications of the Association for Information Systems, 20(57)*, 958 – 971, DOI: 10.17705/1CAIS.02057.

Chopra, A., & Chaudhary, M. (2020). Implementing an Information Security Management System. Security Management Based on ISO 27001 Guidelines. https://doi.org/10.1007/978-1-4842-5413-4.

Dehaghi, M. R. (2016). The relation of information security management system efficiency with organisational agility case study: Isfahan Mobarakeh steel company. *International Journal of Business and Management, 11(8)*, 116, doi:10.5539/ijbm.v11n8p116.

De Lange, J., Von Solms, R., & Gerber, M. (2016). Information Security Management in Local Government. Cunningham, P., & Cunningham, M. (Eds.). (2016). IST-Africa 2016 Conference Proceedings. Dublin, Ireland: IIMC International Information Management Corporation. ISBN: 978-1905824-55-7.

Denscombe, M. (2010). The good research guide for small-scale research projects. Fourth edition. New York, USA: McGraw-Hill Education.

Ebrahimian, J. S. (2012). Organizational agility, response time, and organizational flexibility. National Conference on Entrepreneurship and Management of Knowledge-based Businesses, 13-34.

Gunsberg, D., Callow, B., Ryan, B., Suthers, J., Baker, P. A., & Richardson, J. (2018). Applying an organisational agility maturity model. *Journal of Organizational Change Management, 31(6)*, 13151343, DOI 10.1108/JOCM-10-2017-0398.

Hall, J. H., Sarkani, S., & Mazzuchi, T. A. (2011). Impacts of organizational capabilities in information security. *Information Management & Computer Security, 19(3)*, 155-176, DOI 10.1108/09685221111153546.

Heckler, J., & Powell, A. (2016). IT and Organizational Agility: A Review of Major Findings. MWAIS 2016 Proceedings. 3. Retrieved May 8, 2023, from http://aisel.aisnet.org/mwais2016/3.

Huang, P. Y., Ouyang, T. H., Pan, S. L., & Chou, T. C. (2012). The role of IT in achieving operational agility: A case study of Haier, China. *International Journal of Information Management 32,* 294– 298, doi:10.1016/j.ijinfomgt.2012.02.001.

ISO/IEC 27000 (2014). Information technology — Security techniques — Information security management systems — Overview and vocabulary.

ISO/IEC 27001 (2013). Information Technology—Security techniques—Information security management systems— Requirements.

Johannesson, P., & Perjons, E. (2014). An Introduction to Design Science. Springer International Publishing. https://doi.org/10.1007/978-3-319-10632-8.

Ključnikov, A., Mura, L., & Sklenár, D. (2019). Information security management in SMEs: factors of success. *Entrepreneurship and sustainability issues, 6(4)*, 2081-2094, http://doi.org/10.9770/jesi.2019.6.4(37).

Knapp, K. J., Marshall, T. E., Rainer Jr. R. K., & Morrow, D. W. (2006) The Top Information Security Issues Facing Organizations: What Can Government Do to Help?. *Information Systems Security, 15(4)*, 51-58, DOI: 10.1201/1086.1065898X/46353.15.4.20060901/95124.6.

Latham, J. R. (2022). The Research Canvas: A Framework for Designing & Aligning The DNA of Your Research Study (4th ed.). Organization Design Studio® Ltd. Retrieved May 8, 2023, from https://www.drjohnlatham.com/books/the-research-canvas/.

Leonhardt, D., Mandrella, M., & Kolbe, L. (2016). Diving into the Relationship of Information Technology and Organizational Agility: A Meta-Analysis. Thirty Seventh International Conference on Information Systems, Dublin 2016.

Li, G., Lin, Y., & Yan, H. (2006). Enhancing agility by timely sharing of supply information. International Journal of Supply Chain Management, 11(5), 425-435.

Ma, Q., Johnston, A. C., & Pearson, J. M. (2008). Information security management objectives and practices: a parsimonious framework. *Information Management & Computer Security, 16(3)*, 251-270, DOI 10.1108/09685220810893207.

Ma, Q., & Pearson, J. M. (2005). Iso 17799: "Best practices" in information security management? *Communications of the Association for Information Systems, 15(2)*, 577-591.

Marshall, B., Cardon, P., Poddar, A. & Fontenot, S. (2013) Does Sample Size Matter in Qualitative Research?: A Review of Qualitative Interviews in is Research, Journal of Computer Information Systems, 54:1, 11-22, DOI: 10.1080/08874417.2013.11645667.

Mrugalska, B., & Ahmed, J. (2021). Organizational Agility in Industry 4.0: A Systematic Literature Review. *Sustainability, 13(8272),* 1-23, https://doi.org/10.3390/su13158272.

O'Hair, H.D., & Kreps, G.L. (Eds.). (1990). Applied Communication Theory and Research (1st ed.). Routledge. https://doi.org/10.4324/9780203812204.

Peltier, T. R. (2003). Establishing business controls for electronic mail communications. *Information Systems Security, 12(1)*, 34-43, doi.org/10.1201/1086/43325.12.1.20030301/41479.6.

Purser, S. (2004). A practical guide to managing information security [Elektronisk resurs]. Boston, MA: Artech House.

Ridwandono, D., & Subriadi, A. P. (2019). IT and organizational agility: A critical literature review. Procedia Computer Science, 161, 151-159. https://doi.org/10.1016/j.procs.2019.11.110.

Sambamurthy, V., Bharadwaj, A., & Grover, V. (2003). Shaping Agility through Digital Options: Reconceptualizing the Role of Information Technology in Contemporary Firms. *Management Information Systems Research Center, University of Minnesota, 27(2)*, 237-263, Retrieved May 8, 2023, from https://www.jstor.org/stable/30036530.

Sindhwani, R., Singh, P. L., Iqbal, Prajapati, D. K., & Mittal , V. K. (2019). Modeling and Analysis of Factors Influencing Agility in Healthcare Organizations: An ISM Approach K. Shanker et al. (eds.), Advances in Industrial and Production Engineering, Lecture Notes in Mechanical Engineering, 683-696, https://doi.org/10.1007/978-981-13-6412-9_64.

Singh, A. N., & Gupta, M.P. (2013). Identifying factors of "organizational information security management". *Journal of Enterprise Information Management, 27(5)*, 644-667, DOI 10.1108/JEIM-07-2013-0052.

Singh, A. N., & Gupta, M.P. (2019). Information Security Management Practices: Case Studies from India. *Global Business Review, 20(1),* 253–271, DOI: 10.1177/0972150917721836.

Singh, A. N., Picot, A., Kranz, J., Gupta, M. P., & Ojha, A. (2013). Information Security Management (ISM) Practices: Lessons from Select Cases from India and Germany. *Global Journal of Flexible Systems Management, 14(4)*, 225–239, DOI 10.1007/s40171-013-0047-4.

Stenfors, T., Kajamaa, A., & Bennett, D. (2020). How to… assess the quality of qualitative research. *The clinical teacher*, 17(6), 596-599.

Tan F.T.C., Tan B., Wang W., & Sedera D. (2017). IT-enabled operational agility: An interdependencies perspective. *Information and Management, 54(3)*, 292-303, https://doi.org/10.1016/j.im.2016.08.001.

Von Solms, B., & Von Solms, R. (2004). The 10 deadly sins of information security management. *Computers & Security, 23(5)*, 371–376.

Walter, A.-T. (2021). Organizational agility: ill-defined and somewhat confusing? A systematic literature review and conceptualization. Management Review Quarterly, 71:343–391, https://doi.org/10.1007/s11301-020-00186-6.

Werlinger, R., Hawkey, K., & Beznosov, K. (2008), An integrated view of human, organizational, and technological challenges of IT security management. *Information Management & Computer Security, 17(1)*, 4-19, DOI 10.1108/09685220910944722.

Yin, R. (2009). Case Study Research: Design and Methods (4th ed.). Thousand Organizational Agility ks, CA. Sage.

Zain, M., Rose, R. C., & Masrom, M. (2005). The relationship between information technology acceptance and organizational agility in Malaysia. *Information and Management, 42(6)*, 829-839. http://dx.doi.org/10.1016/j.im.2004.09.001

Zaini, M. K., & Masrek, M. N. (2013). Conceptualizing the Relationships between Information Security Management Practices and Organizational Agility. In International Conference on Advanced Computer Science Applications and Technologies (269–273). Malaysia: CPS - Conference Publishing Services.

Zaini, M. K., Masrek, M. N., & Sani, M. K. J. A. (2020), The impact of information security management practices on organisational agility. *Information & Computer Security, 28(5)*, 681-700, DOI 10.1108/ICS-02-2020-0020.

Appendix A – Consent Form

Participant Consent Form

Title: Managing Information Security while maintaining Organizational Agility **Case Study**: A Financial Institution in Nigeria.

Researcher: Temitayo Eniola Adetona
Email: temithayur@gmail.com
Program/University: Department of Computer and Systems Sciences / Stockholm University Masters in strategic information systems management

I hereby ask for your voluntarily taking part in my master's thesis research project. This study aims to have a deeper understanding of "*How organizations manage information security while maintaining organizational agility and to investigate how organizations develop and implement information security measures that can withstand internal and external threats while retaining organizational agility and highlighting the challenges encountered in the process*".

For participation:

- I willingly consent to take part in this study, and I may decide to withdraw at any time without penalty;
- I've been given explanations about the study's aim and goal;
- I consent to take part in this study and I am aware that it must be submitted as a requirement for the Master's program to the university;
- I understand that every document will be kept private and, in the researcher's safe custody;
- I am aware that any information gathered will only be used for this purpose or other authorized research purposes by Stockholm University;
- I also understand I will not directly gain anything from taking part in this research;
- I may be contacted further by the researcher if additional information is required;
- I consent to the researcher recording my interview;

Please feel free to contact the researcher if you have any questions.

I acknowledge that I have read the following information, and I consent to take part in the study.

Participant's Name:
Date:
Signature:

Appendix B – Interview Questions

Interview Questions	**Motivation**
Introduction of Participants	
• Would you kindly introduce yourself? • How many years have you been with this organization? • Can you give a brief description of what your organization does? • What does your job entail? • Do you hold any security certifications? Please specify.	To get to know the participants, what their jobs entail, and what the organization does
Information Security Management (ISM)	
• What does ISM mean to you? • Does your organization have a specific security steering group in charge of ISM? • Is there Segregation of duties within your Information Security group? • Do you think it's challenging to manage information security at your company? If yes, why? • Could you please identify the essential Information Security concerns within your organization?	To have an overview of what ISM means to the participants, understand how Information Security is being managed in the organization and the challenges encountered in doing that.
Organizational Agility	
• What do you understand by organizational agility, and why do you believe it is crucial in the current corporate environment? • What measures would you suggest taking to make your organization more agile? How might this be accomplished? • How does your organization maintain its agility while managing risk and uncertainty? • How, in your opinion, does your company handle information security while preserving organizational agility? Any challenges?	To have an overview of what Organizational Agility means to the participants with respect to the organization, and how it is being maintained in the face of risk and uncertainty

ISM best practices	

What would you say are the ISM best practices based on your experience?	To have an understanding of the ISM best practices used in the organization
Information security requirements	
• What, in your opinion, is the impact of information security in organizations? • Are there safeguards in place to guard against intrusion and viruses and to maintain the security and integrity of important software and data? • What are the consequences of an Information Security breach in your organization based on your experience? • How soon do you react to Information Security attacks in your organization when there is a breach?	To understand the requirements of Information Security, the consequences of breaches, and how attacks are being reacted to and handled
Top management support	
• In terms of Information Security activities, would you say that senior management always supports your group? What do you think about the support offered? How would you rate it? On a scale of 1 to 10. • When it comes to Information Security activities, do you easily have access to essential resources from the management?	To determine the role of senior management in relation to Information Security as well as the level of participation/support received from them, and mention areas they could improve on
Information security policy	
• Are there Information Security policies in place at your organization? • How frequently do you believe these regulations are being examined for accuracy and efficacy? • Are there sufficient policies and processes in place to operationally uphold the organization's information security standards? If not, what steps are being taken to change that? • Do you think the company's information security policies and standards are working? If not, what steps can be taken to guarantee its efficacy?	To have an overview of the Information Security policies in place, to know the level of its efficacy, and the impact it has had on the organization
Information security training and awareness	

• Does your organization provide staff with Information Security training? If so, how frequently do this training take place? • Do you think the training was beneficial or not? Tell me more about that, please.	To have an understanding of how training and awareness is conducted for the employees, the benefits, the impact it has had, and the challenges encountered
• Is there a committee in charge of training or there is no structure in place? • Does the business have sanctions in place for staff who violate the information security policy? • Does the organization have an Information Security awareness program in place? If so, what does it entail?	
Information security audit	
• Which kind of Information Security audit does the organization conduct? Are they internal, external, or both? What exactly are these auditing procedures, please?	To determine the type of audit carried out in the organization, the challenges experienced, and the auditing procedures in place
Physical and environmental security	
• What physical and environmental security regulations are in place to protect crucial IT facilities? • Are there any safeguards in place to stop the moving of IT equipment without permission?	To understand how physical and environmental security is being handled and how it has been helpful in securing the assets of the organization.

Appendix C – Reflection Document 1

How does your study correspond to the goals of the thesis course? Why? Focus on the goals that were achieved especially well and those that were not well achieved.

The goal of this study is to identify how organizations manage information security while maintaining agility. Organizations keep looking for measures to remain agile and better protect the security of their information. As a result, these measures have been identified which is in line with the goals of the thesis. These measures will help organizations to better achieve their purpose of securing information. However, getting the participants to agree to a convenient time for the interviews was a bit challenging.

How did the planning of your study work? What could you have done better?

Because the thesis was done by only me, this made it a bit easier for me to plan myself based on my schedule which involved staying up late till midnights. It took a while getting used to but eventually, it became less stressful. I had a bit of delay in getting the participants based on their busy schedules. Also, transcribing was a bit stressful and took a lot of time. I would have preferred to subscribe to a paid version of the transcribe app as there are lesser incoherent words when transcribing.

How does the thesis work relate to your education? Which courses and areas have been most relevant for your thesis work?

I study Strategic Information Systems Management and my thesis is on managing information security. I believe that they are closely related because they both have to do with management of Information. Prior to the start of my program, my writing skills was not top notch but with the help of this course - Scientific Communication and Research Methodology (FMVEK), I had more confidence in myself, the course really prepared me. Also, Information Security in Organizations (SECORG) prepared me for the thesis because I gained more knowledge about information security from the course.

How valuable is the thesis for your future work and/or studies?

Having had 7 years of work experience in the IT sector, writing this thesis brought back good memories. I could easily relate with all that was written because I have had first-hand experience on the job. In my future work, I will try to put in practice some of the things that I have learned from the study.

How satisfied are you with your thesis work and its results? Why?

I am very much satisfied with the whole thesis work. I can now confidently write a thesis report. I also appreciate the quick responses provided by my supervisor which helped in concluding my work on time. My result makes me value my colleagues back when I was in the banking industry seeing that a lot is actually involved in ensuring that the information and assets of the organization are well secured.