Chapter One
Introduction

1.1 Overview

Information security relates to an array of actions designed to protect information and information systems". Conversely, information security does not protect only the information, but also the whole infrastructure that makes its use easier. It covers hardware, software, and physical security. The number of applications, users and systems increase, the more the management of an organization’s information security gets more complex and the vulnerability increases. In order to ensure secure use of hardware and software in an organization, the security awareness program, as well as the support of the top management [1].

Firm’s standards overall policy of security measures is the central place where intangibles such as corporate philosophy, culture, attitude to risk and other difficult to identify certain parameters that can finally be crystallized into enforceable, measurable action statements, proceedings and methods of working. The scope of such overall policy affected by the size and nature of the organization activities, but the underlying required a security policy is nevertheless irrefutable.

In addition, security itself is not a product, but a process is necessary to constantly ensure that an organization's security policy still go on in order to face the rapidly changing and evolving needs of the business. Information is one of the essential and Irreplaceable resources are heavily on organizations dependent on. The data of an organization is compromised; the company can suffer the loss of income and loss of customers' trust.

Similarly, the security policy is a group of acceptable habits or exercises arranging the modality organization, protects, assigns and run actual resources to accomplish its direct security objectives. This combination of the institution's aims and security objectives underlie the management controls that are applied in nearly all business practices to reduce the risks that gathered with a false and human error [1].

1.2 Problem Background

Effective security policies vary greatly depending on the nature of the organization activities. This remains effective regardless of the volume of the organization to which apply, receive attention. Whatever the volume of an organization, and whatever its present situation of information security overall policy, there is always objective behind for a salutary check of existing policy and procedures from time to another. The organizations must take active steps to preserve the security and impartiality of their information resources and now here is this strategy more critical than in Public sectors in Sudan where issues of information accuracy and public sector confidentiality are paramount of all the tools at the information security manager's disposal, none is more widely valued and used than the information security policy. Such a task is legal and necessary or unsuccessful to explore alternative views of general workable security policies.

Many organizations do not have their own resources or and skills to achieve a risk analysis assignment fully and accordingly to carry out an ISMS. Therefore, they might not know which security aspects might be. Therefore, might not know which security aspects might be relevant to them. Instead of doing a full risk analysis, an Organization could also look at its peers. What do they do? Although following your peers might not be perfect as doing an extended risk analysis, it is certainly better than implementing controls

without any reason at all. Modern times call for different approaches to problems [2].

1.3 Problem Statements

Lack of information security policies framework having been identified as one of the main factors that contribute to the slow progress in the implementation of information security measures in institutions including those in the public sector this study is seeking to identify the obstacles facing the public sector in Sudan .

1.4 Objectives of the Study:

- To survey the effectiveness of information security policies and application at the public sector entities and come.
- To improve the effective information security policy and practices at Sudanese public sector.
- To develop the performance of security policy in government institutions region and the public sector.

1.5 Scope of the Study

Effective information security policy was a program within most organizations. More effective examined and assessed the efficacy of information security policies and application at the public sector entities and come, and recommend solutions and guidelines to improve the development the effectiveness of information security frameworks and practices at Sudanese public sector and enhance the performance of the community sector.

1.6 The Proposed Solution

The security policy must include guidelines and standards that attempt to eliminate the common kinds of attacks that threaten most companies. The

policy tries to deduce and identify workable solutions that supplying an agreeable stage of security measurement. The research method used in this research study is qualitative methods and quantitative method, so-called mix mode and create a code applied to the server, which checks the policies applied to the network.

1.7 Structure of the Thesis

Chapter two Literature reviews: This chapter provides broad concepts like information security policy and its frameworks. Provides an overview of policies, standards and practices. The success factors related to the implementation of information security in organizations are explained. It ends with a summary of the different theories used in this study. Chapter three Methodology: This chapter explains the research methods that were used in this study. It starts with a research philosophy and explains in details the research approach, Interviewees and research strategy. By then the explanation of data collection and data analysis. Moreover, the validity and reliability of the research are discussed, and some ethical considerations are underlined. Chapter four Finding and survey Results: This chapter provides all the data that was collected using the questionnaire. This chapter provides an analysis of the findings. Chapter five conclusion and recommendations are the last chapters of this thesis. It concludes the research by answering the research questions. It also defined specific recommendations to the effectiveness of information security policies.

Chapter Two

Literature Review

2.1 introduction

Information is a critical asset of the government and citizens, and the information was converted into digital formats; it has become imperative that the Government implements a sound operational information security policy to protect its information assets. Knowledge expanded based on the previous research is refutable and consistent. Consequently, the very first step towards the solution research problem is to overview the findings of previous research. For this purpose, this chapter reviews the publications and literature. Different themes are identified from the previous studies here.

2.2 Concept of Information and Communication Technology

The growth of Information and Communication Technology (ICT) has been so explosive in the recent decade. The computer has been widely applied in every aspect of life from business, government, education, finance, healthcare, and aerospace to the defence system. With society's increasing dependence on Information Technology (IT) [3], this sense must identify some concepts such as Data, Information and Technology and Data which plain facts. The word "data" is plural for "datum." When data are processed, organized, structured or presented in a given context so as to make them useful, called Information.

Information is data that has been processed in such a way as to be meaningful to the person who receives [4]. Technology is the application of knowledge and skills to make goods or to provide services. Communication for many companies, email is the principal means of communication between

employees, suppliers and customers. The email was one of the early drivers of the Internet, providing a simple and inexpensive means to communicate.

The main role that is played by communication networks is called ICT has an important, prominent role in knowledge due to its changeable ability and its capability of making the relationship among organizations [5].In the past few decades, information and communication technologies have provided society with a vast array of new communication capabilities. For example, people can communicate in real-time with others in different countries using technologies such as instant messaging, Voice over Internet Protocol (VoIP), and video-conferencing and social networking websites like Facebook allow users from all over the world to remain in contact and communicate on a regular basis.

Modern information and communication technologies have created a "global village" in which people can communicate with others across the world. ICT is often studied in the context of how modern communication technologies affect society [6].

2.3 Information Security

Nowadays, security is becoming a number one priority for governments, organization, companies, and individuals. Security is all about protecting critical and valuable assets. Protecting valuable and critical assets, whether tangible or intangible, is a process that can be ranged from being unsophisticated to be very sophisticated. What is Security? Security is quality or state of being secure to be free from danger". A successful organization should have multiple layers of security in place:

- Physical security
- Personal security
- Operations security
- Communications security
- Network security

The protection of information and its critical elements, including systems and hardware that use, store, and transmit that information.Necessary tools for security: policy, awareness, training, education and technology [7].

2.4 Definition of Information Security Policy

Organizations need to know the value of information, the value of information comes from the characteristics it possesses: Availability (enables user access to information without interference or obstruction), Accuracy, Authenticity (proof that a user possesses the identity), Confidentiality,Integrity,Utility (valuable), Possession (ownership) and how it can be compromised in order to develop protective measures.

Figure 2.1: Confidentiality, integrity, and availability (CIA Triangle) [8].

This Figure 2.1There is a general consensus as to the meanings of confidentiality, integrity, and availability (C.I.A) Triangle was standard based on:

Availability: The prevention of unauthorized withholding of information or resources. This does not apply just to personnel withholding information. Information should be as freely available as possible to authorized users.

Integrity: The prevention of erroneous modification of information. Authorized users are probably the biggest cause of errors and omissions and the alteration of data. Storing incorrect data within the system can be as bad as losing data. Malicious attackers also can modify, delete, or corrupt information that is vital to the correct operation of business functions.

Confidentiality: The prevention of unauthorized disclosure of information. This can be the result of poor security measures or information leaks by personnel. An example of poor security measures would be to allow anonymous access to sensitive information.C.I.A. triangle now expanded into a list of critical characteristics of information: Confidentiality, Authentication, Access Control, Integrity, Non-repudiation, and Availability.

Table (2.1) C.I.A. Triangle critical characteristics

Characteristics	Definition
Confidentiality	To keep a message secret to those that are not authorized to read it
Authentication	To verify the identity of the user/computer
Access Control	To be able to tell who can do what with which resource
Integrity	To make sure that a message has not been changed while on Transfer, storage, etc
Non-repudiation	To make sure that a user/server can't deny later having participated in a transaction
Availability	To make sure that the services are always available to users.

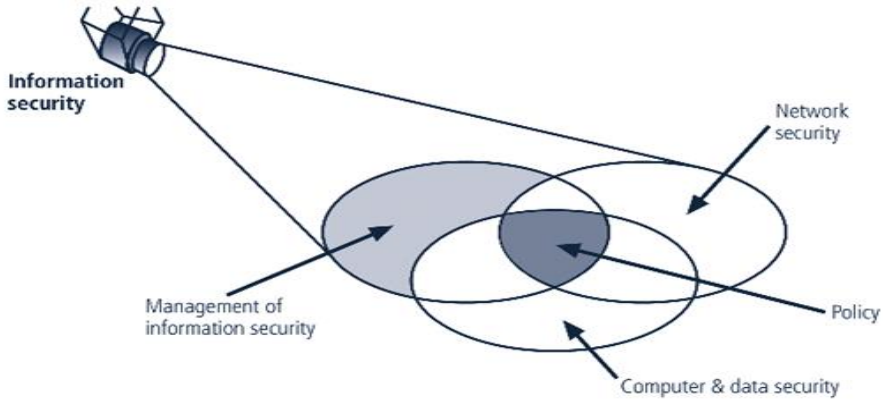

Figure 2.2: Components of information security [9].

Figure 2.2 shown information security is a set of strategies for managing the processes, tools and policies necessary to prevent, detect, document and counter threats to digital and non-digital information. A policy is a deliberate system of principles to guide decisions and achieve rational outcomes to components of information security.

2.4.1 Information Policy

The policy is an essential foundation of the effective info-sec program, the success of an information resources protection program depends on the policy generated and on the attitude of management toward securing the information on automated systems.

A statement of intent, and is implemented as a procedure or protocol. Policies are generally adopted by a governance body within an organization. The information security policy is a direction-giving document for information security within an organization. It is a document that indicates management's commitment to and support of information security, as well as defines the role information security has to play in reaching and supporting the organization's vision and mission [10].

The policymaker set the tone and the emphasis on how important a role info-sec within agency. Also as the policy maker primary responsibility is to set the information resource security policy for the organization with the objectives of reduced risk, compliance with laws and regulations and assurance of operational continuity, information integrity and confidentiality."

These basic rules to follow when shaping policy:

- Never conflict with the law
- Stand up in court
- Properly supported and administered
- Contribute to the success of the organization
- Involve end users of information systems

The following Bull's eye model is the information security program that focuses on the role of policy. It contains four main layers.

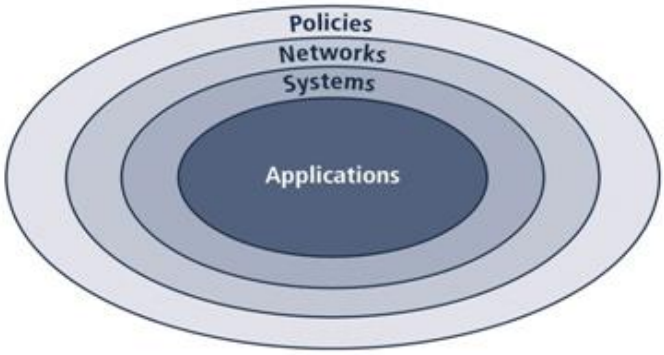

Figure 2.3: Bulls-eye model layers [11]

Figure 2.3 Explain Bulls-eye model layers:

Policies: a first layer of defence

Networks: threats first meet organization's network

Systems: computers and manufacturing systems

Applications: all applications systems

Policies areimportantreferenceand documents for internal audits and for resolution of legal disputes about management's due diligence, policy documents can act as a clear statement of management's intent.

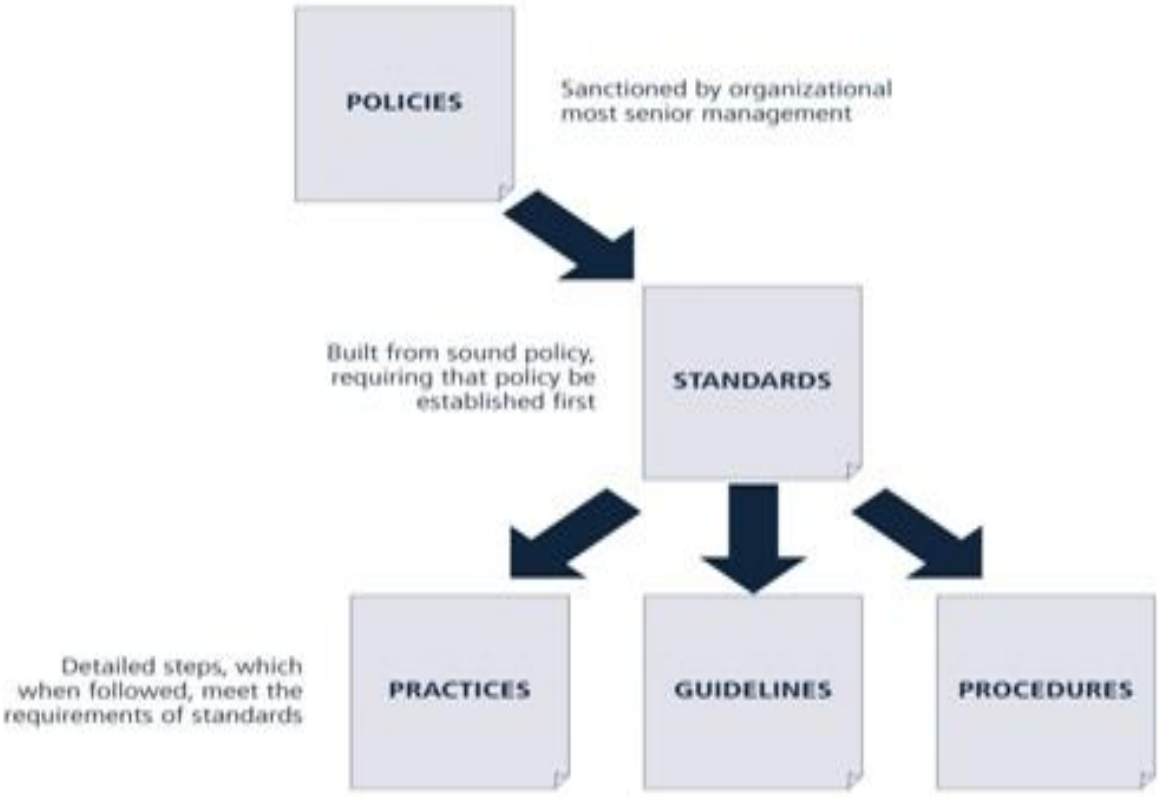

Figure 2.4: policies, Standards and Practices [11].

Figure 2.4 Explain policies, Standards and Practices:

Policy: plan or course of action that influences & determines decisions.

Standards: a more detailed statement of what must be done to comply with the policy.

Practices, procedures and guidelines: explain how employees comply with the policy.

For policies to be effective there are:

Properly disseminated

Read

Understood

Agreed-to

Information security policy documented to explain the need for information security and its concepts to all of the organization's information resource users. It should complement the organizations. Business objectives and reflect management's willingness to operate the organization in a controlled and secure manner.

2.5 Information Technology security frameworks

Information security framework is a series of documented processes that are used to define policies and procedures around the implementation and ongoing management of information security controls in an enterprise environment. These frameworks are a "blueprint" for building an information security program to manage risk and reduce vulnerabilities [12].

Information security pros can utilize these frameworks to define and prioritize the tasks required to build security into an organization. Frameworks are often customized to solve specific information security problems, just like building blueprints are customized to meet their required specifications and use. There are frameworks that were developed for specific industries as well as different regulatory compliance goals. also come in varying degrees of complexity and scale. However, find that there is a large amount of overlap in general security concepts as each one evolves.

Information security frameworks are a collection of standardized policies, procedures and guides, meant to direct a firm or any organization, which adopts its use, on how to protect its hardware, software, data, information, network, computing devices, users and clients from potential security breaches through their use of the firm's resources or services[13].

There are three main reasons for using the information security frameworks:

Ensure legal compliance with the country of operations Data Protection Act.

Assure customers of their personal data safety and privacy.

Protect the entire firm from network security breaches and invariably, company's data breach.

There are several frameworks available which help in addressing key information security concerns like the popular ones listed below:

Control Objectives for Information and Related Technology (COBIT): A product of vendor-independent organization IT governance professionals. Its key point of focus is on reducing technical risks in an organization.

ISO 27000 Series: This was developed by the International Standards Organization and offers a much wider coverage over a company or organization's processes. It can also be applied to all types and sizes of organizations.

Illustration of a security policy, driven by the ISF mentioned above, is made up of sections or domains which address the company's operational processes or infrastructure as follows:

Security Policy Scope: This addresses the coverage scope of the security policy document and defines the roles and responsibilities to drive the document organizational-wide.

Organizational Security: This addresses the organization's security needs covering its staff, customers or clients, suppliers and other vendors handling key processes on its behalf.

Risk Assessment and Treatment: This helps define potential risks and subsequent responses to reduce its effect on the organization.

Asset Classification: The value of an asset determines the level of sophistication its protection would be. In order to implement this, the company's assets irrespective of its size or use are classified and protected.

Human Resources Security: This deals with the processes involved with staff engagement, on-boarding and termination processes.

Physical and Environmental Security: Protection of the firm's building and physical entry access, as well as protection of the environment from the dangers which could have an impact on the building itself.

Communications and Operations Management: This section addresses the communication and operational channels of the organization. Protecting each channel on a need to know and access basis.

System Access Controls: This addresses the requirements and standards for the granting and maintenance of access to staff on systems, applications, and network.

System Development and Maintenance: This deals with the development of new systems, maintenance of existing ones and evaluations of security controls in line with changes affected in the system.

2.6 Related Work

The Related work used in this research is concentrated on the related areas with information security policy, security awareness and training, the effectiveness of information security policy in the public sector, researchers have developed many methods and tools for how to make information security policy and procedure effectiveness and there are some articles which are related to our work.

In [2] reported that Information security systems in special and public libraries

aimed to determine the implementation status of technological and Organizational Components of the framework model. Implementation index, as well as a scoring tool, is presented to assess the IS safeguarding measures in a library. Data used was based on questionnaires and distributed to in the special and public libraries in Malaysia. Findings revealed that over 95% of libraries have a high level of technological implementation. However, 54% were fair poorly on organizational measures, especially on lack of security procedures, administrative tools and awareness creation activities.

The [4] studied the directed of the research is a novel model shows how complying with organizational information security policies shapes and mitigates the risk of employees' behaviour. The significant aspect of this research is derived from the conceptualization of different aspects of involvement, such as information security knowledge sharing, collaboration, intervention and experience, as well as attachment, commitment, and personal norms that are important elements in the Social Bond Theory.

In [5] reported that a management practice perspective. The aimed of the research is provides a comprehensive overview of the management practices of information security policy and develops a practice-based model. The model provides comprehensive guidance to practitioners on the activities security managers must undertake for security policy development and allows practitioners to benchmark their current practice with the models suggested best practice. The model contributes to theory by mapping existing information security policy research in terms of the defined management practices.

In [6] it investigated the effectiveness, vulnerabilities and threats. The aimed of the research are on the issue of information security policy for e-government in Saudi Arabia. It evaluates the three fundamental pillars that determine data security, such as effectiveness, vulnerabilities, and threats. The

paper is seeking to reveal the risks of information security policy for e-government in Saudi Arabia as well as to examine the vulnerabilities and the effectiveness of the system. The methodology applied inductive approach where both qualitative and quantitative research method was used. A survey by use of questionnaires and an interview was conducted.

The [19] talked over the aimed of the research to investigate what countermeasures for information security threats organizations typically use, and how to select such countermeasures. Although many prescriptive documents on ISO 27002 exist, this research combines both previously named aspects into a descriptive overview of what controls typically are used, how selected and how the interviewed practitioners think should be selected. The two biggest issues found in this research were lack of management commitment and lack of employees' understanding of information security.

The [15] reviewed 114 influential security policy-related journal articles and identified five core relationships examined in the literature. Based on these relationships, outline a research framework that synthesizes the construct linkages within the current literature. Building on their analysis of these results identified a series of gaps and drew on additional theoretical perspectives to propose a revised framework that can be used as a basis for future research.

In [20] reported that the aimed of the research in this study information security awareness training is realized. The level of awareness among the participants in regard to information security is assessed and measured before and after the awareness training. The purpose of this is to let the effectiveness of the awareness training be highlighted, shown, and to find out to what extent it is effective. The methodology used to accomplish this task is online surveys and interviews.

In [21] studied information security and provides an overview of general

information security concepts, recent evolutions, and current challenges in the field of information security.

In [22] debated changes and implications for personal data collecting companies aimed to review and thematic analysis and synthesis of the article-level changes were carried out. Through the analysis, the key practical implications of the changes were identified and classified. As a synthesis of the results, a framework was developed, presenting 12 aspects of these implications and the corresponding guidance on how to prepare for the new requirements. These aspects cover business strategies and practices, as well as organizational and technical measures.

[27]reported that the article addresses the elements that make up a successful information security awareness program. It addresses the role that organization personnel play in the information security program and how to use this information to one's benefit. It also discusses how to establish an awareness program scope, how to segment the audience, and how to ensure that the content is effective in getting the message to the user community.

In [36] reported that propose a framework to cultivate an information security culture within an organization and to illustrate how to use it.The empirical study is performed to aid in validating the proposed information security culture framework.

In [37] discussed taken on increasing importance as the size and complexity of IT issues continue to grow. In this research, the framework was analyzed defining how the three constructs: security policies, deterrence practices and systems auditing impact information security effectiveness. A survey was conducted to collect data, the results of which suggest that there is a significant relationship between security policies and systems audit with security effectiveness.

In [38] argued focuses on one such threat the co-resident attack, where malicious users build side channels and extract private information from virtual machines co-located on the same server. It chooses to solve the problem from a different perspective, by studying how to improve the virtual machine allocation policy, so that it is difficult for attackers to co-locate with their targets. Specifically, it defines security metrics for assessing the attack, model these metrics, and compare the difficulty of achieving co-residence under three commonly used policies. Design a new policy that not only mitigates the threat of attack, but also satisfies the requirements for workload balance and low power consumption; and implement, test, and prove the effectiveness of the policy on the popular open-source platform Open Stack.

In [39] discussed the exceptions that are provided in the standard contractual clause and the reason behind the transition from Safe Harbor .

This article subsequently embarks on the concept of Binding Corporate Rule, which was introduced by the working party and how the new regulation has viewed this internal rule regarding assisting cross-border data transfer. All the issues that discussed in this article are relevant in the understanding of cross-border data transfer.

In [40] reported that this study uses the two frameworks: COBIT 5 and IT Security for Information Technology Audit. The Information Technology audit results of the institutions have the maturity level of information technology management at level 2 are Repeatable but Intuitive controls for mapping and principle of COBIT 5, while the average score of information security standard ISO/IEC 17799:2005 was 39%. The results of data processing to find the average for the maturity level of information security standard ISO/IEC 17799:2005 is 31 or 39%, which means that the security of information technology is still very less and should be highly improved .

The [41] reviewed the aimed of the research in this field is to determine in what way can improve our prediction abilities. An important goal of this paper was to develop an evaluation model, which would allow such comparisons. For this purpose, developed an agent-based simulation model which measures the exposure of information system to exploitable vulnerabilities. Besides, some policies which take into account human threats were defined and then compared with the most popular existing methods. Experimental results imply that the proposed policy, which is based on attacker characteristics, achieves the highest efficiency among existing methods.

Table (2.2) Summary of Related Works

Study	**Objective**	**Method**
(Safa, 2016)[4].	the conceptualization of different aspects of involvement	a novel model shows how complying with organizational information security policies shapes and mitigates the risk of employees' behaviour
(Alshaikh, 2016) [5].	Discusses the management practices of information security policy	provide a model which contributes to theory by mapping existing information security policy research regarding the defined management practices.
(Khaled, 2015) [14].	The paper evaluates the three fundamental pillars that determine data security such as effectiveness, vulnerabilities, and threats.	An inductive approach where both qualitative and quantitative research method was used. A survey by use of questionnaires and an interview was conducted.
(Dobrovoljc2017)[18].	The aimed of the research in this field is to determine in what way can improve our	develop an agent-based simulation model which measures the exposure of information system to exploitable

	prediction abilities.	vulnerabilities
(PimSewuster, 2010) [19].	The research of this thesis aims to investigate what countermeasures for information security threats organizations typically use, and how select such countermeasures	A descriptive overview of what controls typically are used, how selected and how the interviewed practitioners think should be selected.
(Veseli, 2011)[20].	The level of awareness among the participants regarding information security.	online surveys and interviews, to assess the level of awareness among the participant before and after the awareness training.
(Thomas 2010)[31].	The article addresses the elements that make up a successful information security awareness program	It addresses the role The paper discusses each element and its importance.

2.7 Summary

This chapter has provided an overview of the concept of ICT and information security policy and how organizations embrace information technology in their day-to-day operations, there is a need to assure the security of the information and the infrastructure through which the information was made available making up ICT resources. Efforts directed towards information security, policies developed with information security in mind, and regulations requiring specific types of information security activities in specific industries could all contribute to the assurance of the security of the IT resources.

Chapter Three

Methodology

3.1 Introduction

This chapter describes the methodology that has been used in this research, the strategy to analyze the impact of the effectiveness of information security policies in the public sector and the research location, research method, data collection, sample and population, sample size and research flow chart.

3.2 Research Design

The current study have identified and proved that governmental institutions, firms and technological issues that directly affect the information security measurements and practices [14] in public sector in Sudan, which are suffering from lack of education, training, and awareness of the staff about information security [15] otherwise there is obviously inadequate training of employees who are dealing with e-services. So the Sudanese government must give priority to the awareness programs. Moreover, to reduce security menaces to the information set that shared via internet also, the infrastructure development needs to be redeveloped continuously as the defiance to information security are rapidly changing. Furthermore, there are some suggested solutions to meet the process of enhancing and developing of information security. The database for this research depends on the public sector in Sudan and compiled via primary source.

3.3 Block Diagram:

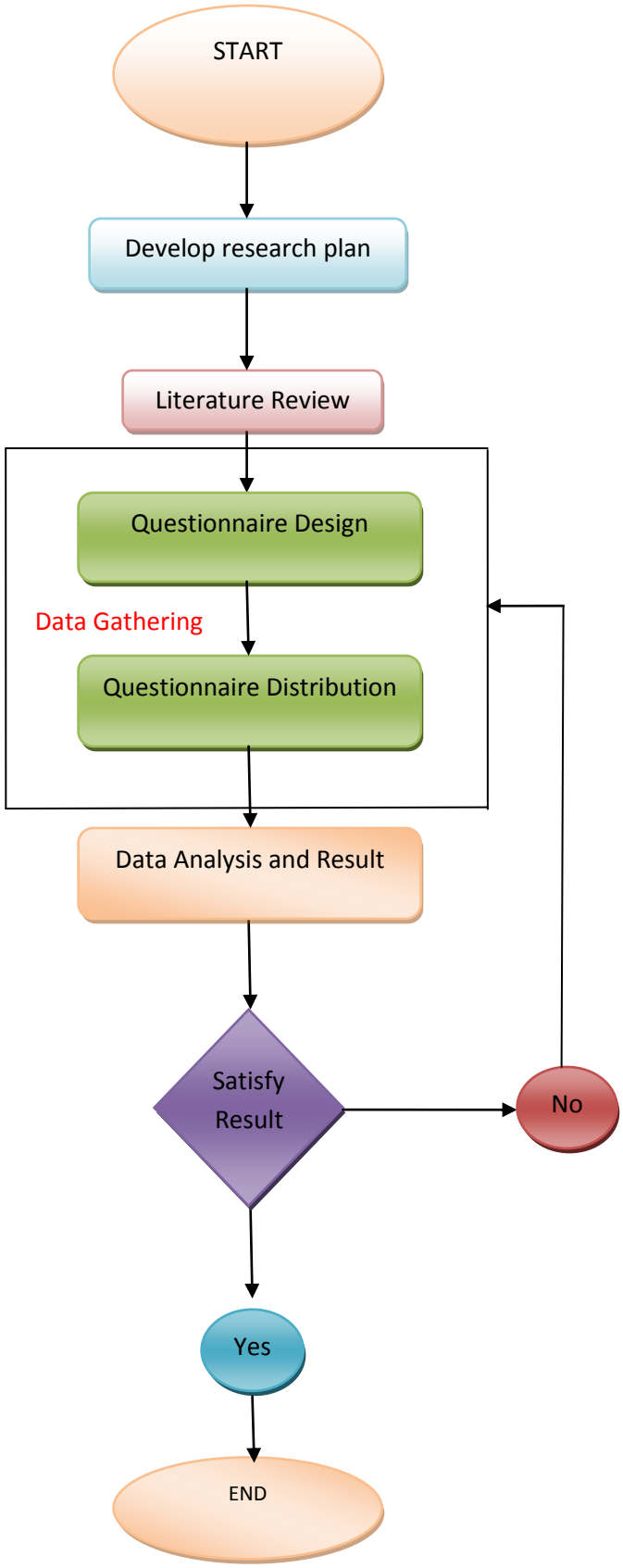

Figure (3.1): Research Methods block diagram.

Figure (3.1) describes the research methods block diagram, which leads to achieving its objectives. The first phase of this research included a summary of a comprehensive literature review. The literature on the effectiveness of the information security policy was reviewed.

The second phase included designing the study questionnaire to be used in examining the impact of the effectiveness of information security policy in Sudan. The third phase of this research focused on distributing the questionnaire to a pilot study. The purpose of the pilot study was to test and prove that the questionnaire questions are clear to be answered in a way that helps to achieve the study objectives.

The Questionnaire validity and reliability tests were conducted for this purpose. The fourth phase focused on distributing the questionnaire among the study population after ensuring its validity and reliability. The fifth phase was data analysis and discussion. The final phase includes the contribution used code was applied to the server, which checks the policies applied to the network, whether it is implemented or not, conclusion and recommendations.

3.4 Research Location

Location of this research based on three public sectors, located in Khartoum for the management interview, and for the customer's interviews conducted inconvenience places in Khartoum Area. This research started in June 2018 and completed in November 2018.These institutions include: the firms were drawn from the three main categories of the public sector, i.e. Ministry of Telecommunication and Information Technology, Ministry of Finance, the National Center of Information and Bank of Sudan.

3.5 Research Method

This research used the descriptive, analytical approach which tries to describe and evaluate the effectiveness of information security policies in the public sector in Sudan. This approach satisfies the research goals in order to compare and evaluate the results, raising our hopes to publicize meaningful content to support the available knowledge of the research theme.

Qualitative Research is primarily exploratory research. It is used to gain an understanding of underlying reasons, opinions, and motivations. It provides insights into the problem or helps to develop ideas or hypotheses for potential quantitative research. Qualitative Research is also used to uncover trends in thought and opinions and dive deeper into the problem. Qualitative data collection methods vary using unstructured or semi-structured techniques. Some common methods include focus groups (group discussions), individual interviews, and participation/observations. The sample size is typically small, and respondents are selected to fulfil a given quota [16].

Quantitative Research is used to quantify the problem by way of generating numerical data or data that can be transformed into usable statistics. It is used to quantify attitudes, opinions, behaviours, and other defined variables – and generalize results from a larger sample population. Quantitative Research uses measurable data to formulate facts and uncover patterns in research. Quantitative data collection methods are much more structured than Qualitative data collection methods. Quantitative data collection methods include various forms of surveys – online surveys, paper surveys, mobile surveys and kiosk surveys, face-to-face interviews, telephone interviews, longitudinal studies, website interceptors, online polls, and systematic observations [17].

In this research, a quantitative part includes paper distribution was used. In addition to direct personal interviews, this is called a qualitative part. A

realistic assessment of gathered data qualitatively is a three-step process that includes data gathering and reducing, displaying results of the analysis, and drawing a conclusion. A measurement scale with response categories ranging from “strongly disagree” to “strongly agree”, which requires the respondents to indicate a degree of agreement or disagreement with each of a series of the statement related to the stimulus objects.

3.5.1 Data Collection Method

The data from this research are collected from various sources. Collected primary data and secondary data required to conduct this thesis. Data collection method used in this thesis was as below:

Questionnaire

The questionnaire is a structured technique for data collection that consist of a series of question, written or verbal, that a respondent answers. The questionnaire was based on the nature of target respondents and the objectives to be achieved.

Questionnaire design

The survey consists of many questions and works related questions.

جامعة السودان للعلوم و التكنلوجيا - كلية الدراسات العليا - ماجستير تقنية المعلومات

استمارة استبيان (-----------)

التاريخ / / 2108 الرقم : .....

إيماناً منا على دور البحث العلمي في التقدم ،أضع بين أيديكم هذه الإستبانة وهي إحدى المتطلبات الدراسية للحصول على درجة الماجستيرعلوم الحاسوب و تقنية المعلومات تخصص شبكات ، بعنوان فعالية سرية امن المعلومات في القطاعات العامة و الهدف من البحث لتقييم فعالية سياسات أمن المعلومات وتحسين وتطوير في القطاعات العامة . وحيث أنني أؤمن بأنكم خيرمصدرللمعلومات المطلوبة ، وأعهدبكم الاهتمام والاستعداد لمؤازرة الأبحاث العلمية التي تهتم بخدمة مجتمعنا وتطويره،لذا توجهت إليكم وكلي أمل في أن أجد التعاون المطلق منقبلكم وذلك من خلال الإجابةعلى أسئلةهذه الإستبانة. أرجومن سيادتكم التكرم بقراءة كل فقرة بعناية و وضع إشارة X أماماالاختيارالمناسب للوصول إلى نتائج دقيقة وموضوعية علماً بأن الإجابة ستعامل بسرية وتستخدم لغرض البحث العلمي فقط ، شاكراً لكم حسن تعاونكم.

اسم الباحث / نور محمد عثمان الامين **ت:0911158929**

أولا :بيانات أساسية:

الاسم: (اختياري) .....

1. المؤسسة:	☐			
2. الجنس:	☐ ذكر		☐ أنثى	
3. الوظيفة	☐	☐	☐	☐اخري
4. المهنه	☐ مدير عام	☐ مدير IT	☐ مهندس	☐ تقني
5. سنوات الخبرة	☐ 5 سنوات فأقل	☐ من 6-10	☐ أكثر من 10 سنوات	
6. العمر	☐ أقل من 35	☐ 35-45	☐ أكثر من 45	

ثانيا: أسئلة الاستبيان :

م	العبارات	درجة التوافر				
		عالية جدا	عالية	إلى حد ما	منخفضة	منخفضة جدا
1	Does the organization have a written information security policy? هل لدى المنظمة سياسة أمن معلومات مكتوبة؟					
2	Is information security policy approved by the top management? هل يتم اعتماد سياسة أمن المعلومات من قبل الإدارة العليا؟					
3	Is the information security policy communicated, to all employees? هل يتم إبلاغ سياسة أمن المعلومات لجميع الموظفين؟					
4	Does the organization have a dedicated information security team? هل لدى المنظمة فريق مخصص لأمن المعلومات؟					
5	Does the informationuseful to conduct an information security awareness program for employees? هل تستخدم المعلومات لإجراء برنامج التوعية بأمن المعلومات للموظفين؟					
6	Does the organization implemented information security solutions: Firewall at intent gateways, Anti-virus - anti-spam هل نفذت المنظمة حلول أمن المعلومات : The firewall at intent gateways, Anti-virus - anti-spam					
7	Does the organization have any procedure to update and batch computer OS and anti-virus? هل لدى المنظمة أي إجراء لتحديث نظام تشغيل الكمبيوتر ومكافحة الفيروسات؟					
8	Does the organization have any user access control policy?					
9	Does the organization have a password policy? هل لدى المنظمة سياسة كلمة مرور؟					
10	Does the organization have any user's access review policy? هل لدى المنظمة سياسة مراجعة الوصول لأي مستخدم؟					
11	How frequently per year the access review is conducted?					

					كم مرة يتم إجراء مراجعة الوصول( )access review في كل عام؟	
					Is the top management supporting and enforcing information security policy implementation? هل الإدارة العليا تدعم تنفيذ سياسة أمن المعلومات وتنفذها؟	12
					Does the organization following any information security standards or guideline? هل تتبع المنظمة أي معايير أو مبادئ توجيهية لأمن المعلومات؟	13
					Does the organization have cybersecurity incident response plan? هل لدى المنظمة خطة استجابة للحوادث الأمنية على الإنترنت؟	14
					Does the organizationimplement any business continuity program? هل تقوم المنظمة بتنفيذ أي برنامج لاستمرارية العمل؟	15
					Does the organization have documented disaster recovery plan? هل لدى المنظمة خطة موثقة لاستعادة القدرة على العمل بعد الكوارث؟	16
					How frequently is the disaster recovery plan tested? كم مرة يتم اختبار خطة التعافي)disaster recovery(من الكوارث؟	17
					Does the organization have any information systems audit program? هل لدى المنظمة برنامج تدقيق لأنظمة المعلومات؟	18
					How frequently is information systems audit conducted? كم مرة يتكرر إجراء تدقيق نظم المعلومات؟	19
					Does the information system audit is part of internal audit responsibility? هل يعتبر تدقيق نظام المعلومات جزءًا من مسؤولية قسم التدقيق الداخلي؟	20
					Can you describe in detail the methods and techniques are used for measuring the effectiveness of information security policies in a sense as to mitigate the threats, vulnerabilities or risk associated withorganizational assets? هل يمكن أن تصف بالتفصيل الطرق والتقنيات المستخدمة لقياس فعالية سياسات أمن المعلومات بمعنى الحد من التهديدات أو نقاط الضعف أو المخاطر المرتبطة بالأصول التنظيمية؟	21
					Do you have a policy monitoring system to monitor and assess your institution network security policies? هل لديك نظام رصد ومراقبة السياساتالامنية وتقيمها لشبكة مؤسستك؟	22

Figure (3-2):Screen Shot Questionnaire Design

Depth Interview

Depth interview is an unstructured, direct, personal interview in which a single respondent is probed by a highly skilled interviewer to uncover underlying motivations, beliefs, attitudes, and feelings on a topic

3.5.2 Data Collection Resources

In order to achieve the research objectives, two essential data collection Resource were used, which are:

Primary Resources: in order to address the analytical aspects of the research theme, the research resorted to collect the primary data through the questionnaire as the main tool, which is designed especially to meet the research objectives. This questionnaire was distributed among the study population, (70) employees working at the public sector s in Khartoum from all three locations received the questioner. Also, personal interviews were conducted with all subjects in order to get their opinions about examining the impact of Effectiveness information security policies in the public sector in Khartoum. Public sectors were subjected to the study.

Excel 2013 was utilized for data analysis, and configured the Network monitoring services and creates a script to check authorization and authentication. The targeted employees at these institutions were from the IT and information archiving departments.

Secondary Resources: in order to address the theoretical background of the study, it has been found on the secondary data collection resources, the likes of books, papers, journals, research studies and finally by surfing the internet to the related websites, it has been found that the main issues are related to the awareness of the importance of having a solid information security policy, having both managers and employees committing to enforce and implement those policies and regularly enhance those policies to meet the main institution goals.

3.6 Research Population

The population of this study is the Public sectors in Sudan. The research has focused on the staff responsible for information technology, computer-based and information archiving departments in those institutions because it discussed the effectiveness of Information Security from a managerial perspective. A comprehensive survey method was used to apply this study on the Governmental Institutions in Sudan, in which this population consists of (76) employees in a variety of job levels working in departments, such as information technology, computer-based and information archiving departments.

3.7 Sample Size

This sample size was calculated to have an 8 % error margin the positive and negative deviation allow on survey results for the sample, and a confident level of 81 % it tells us how sure can be that between 73 % and 89% of the public sector execute an effective information security policy. Considering those parameters and assuming a 77 % response rate or sample size would be 70 subjects distributed throughout 3 ministries, 6 of which are managers and 48 are IT employees who are responsible for the execution of the information security policies in those ministries.

3.8 Data Analysis Methods

Data analysis is said to be the examination of the data that has been collected in research and making deductions and inferences. It involves the scrutiny of collected information and making inferences. This study intended to use confirmatory data analysis method, which makes use of probability theory in the effort to answer particular questions [18].

Assuming a range from 0 to 100%, 0% being the company has no information security policy in place, and no there is no policy being developed or

considered and 100% being that the company already has an information security policy in place and being monitored regularly and evolving with the development of technology.

3.9 Summary

In this research, the collected data has been studied from those two points to evaluate the effectiveness of the information security policy in the companies under study and used descriptive analytical approach and intended to use confirmatory data analysis method which makes use of probability theory in the effort to answer particular questions which try to describe and evaluate the effectiveness of information security policies in public sector in Sudan. Data for the case of Sudan is collected via primary source, and the instruments are questionnaire survey (quantitative part) and face-to-face Information Security Policy for public sector in Sudan: Effectiveness, Vulnerabilities and Threats 70questioner and 3 Interviews were conducted (qualitative part). Quantitative data analysis includes frequency distribution, clustered bar graphs, and pie charts. Analysis of qualitative data is a three-step process that includes reducing the data, displaying the data, and verifying or drawing a conclusion.

Chapter Four

Findings and Discussion

4.1 Introduction

This chapter highlights the statistical techniques an explanation of the participants in this study starting from the analysis of gender and education level and the participants‟ occupation after that come to the analysis of the questionnaire items and interview questions. The results of the data analyzed come in the final of this chapter. In addition, this chapter describes the used techniques in testing the research.

4.2 Participants Backgrounds Analysis

This section analyses the participants whom took part in this questionnaire in different aspects first the gender of the participants taken part in this study, second the occupation of the participants because it is significant to know their work background, third the year of experience of each participant because it is also important to know how long in their work.

4.3 Gender-Based Analysis

Figure (4.1) shows the distribution of genders among the participants in the questionnaire in different institutions as can see the number of male whom participated in the questionnaire is more than the female participants. 26 female from different education level took part in the study, and 28 male also participates from different work experience, after all, it does not matter which gender shows more appearance because all of them are professionals and have several years of experiences in ICT field and Information Security.

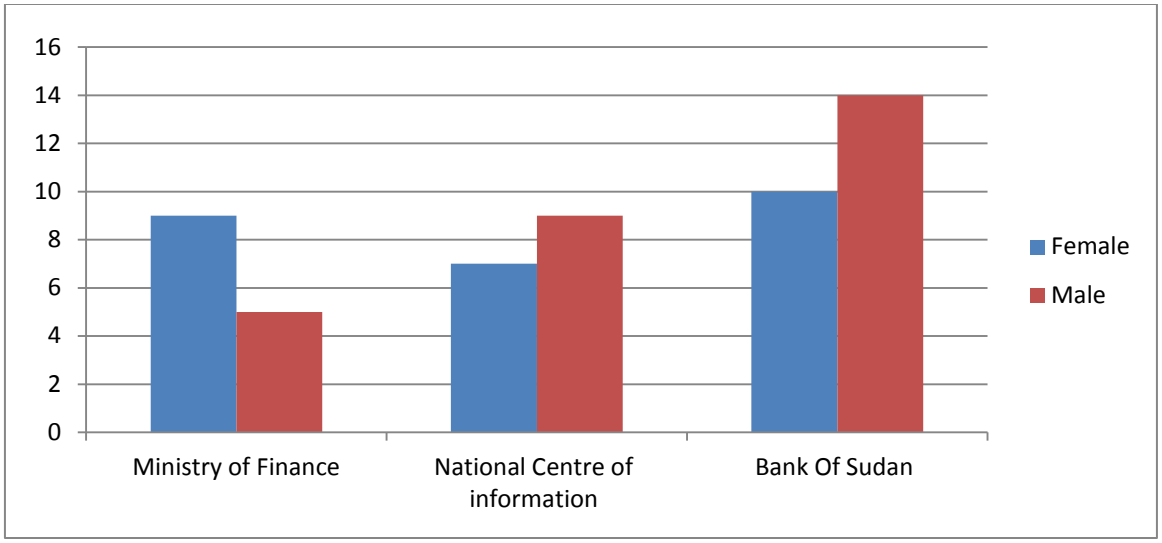

Figure (4.1): Distribution of Gender

4.4 Participants Occupation Analysis

Figure (4.2) shows the actual occupations of the questionnaire participants the majority of the participants are Technicians. Engineers also appeared in this study and IT manager. General Manager has a minor appearance in this project. Generally, the majority of professionals who took part in this study are qualified because their field and occupation related to our project title.

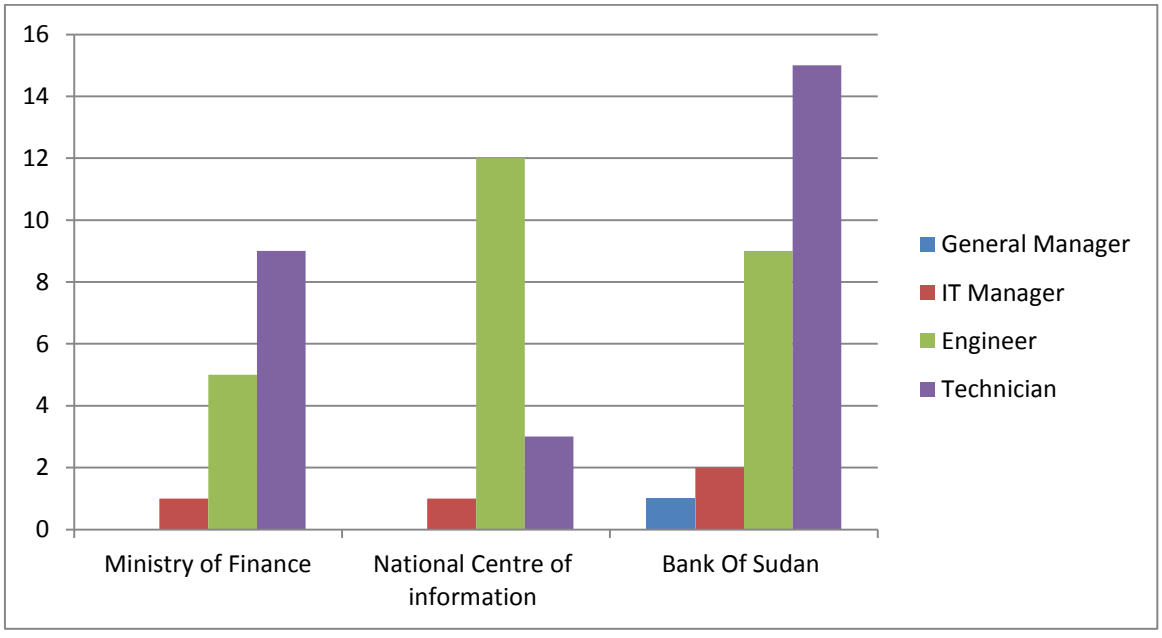

Figure (4.2): Participants' Occupation

4.5 Years of Experiences Analysis

Years of experiences were classified into three-level first from Less than 5 years, second from (6-10) and third Over 10 years. in this study the participants from Less than 5 years has more appearance, after that, the experts from Over 10 years have a good appearance also the professionals from (6-10) years had taken part in this study.

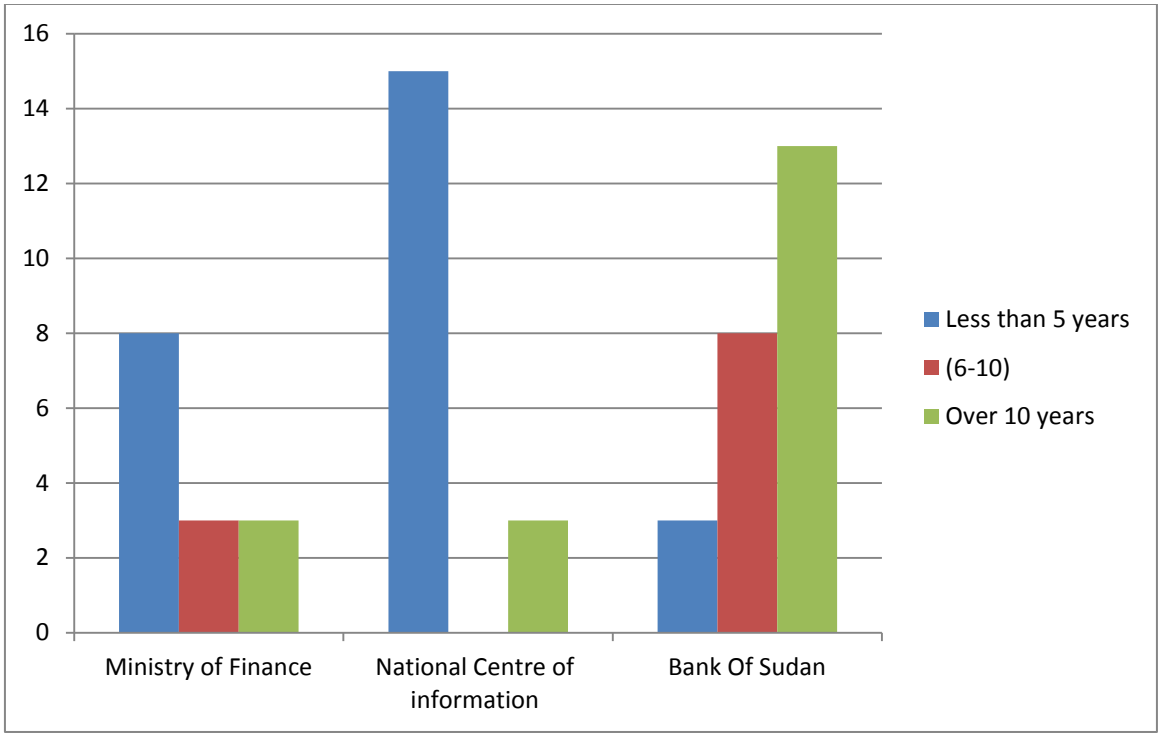

Figure (4.3): Participants' Experiences

4.6 Finding and Results

The distributed survey consisted of 21 statements, all of which were designed to measure the existence of information security policy in three of the major companies representing the public sector in Sudan.

Table (4.1) Research Population's Governmental Institution Representation

Governmental Institution	Frequency	Percent (%)
National Centre of information	16	22.8 %
Ministry of Finance	14	20 %
Bank Of Sudan	24	34.2 %
Total	54	77.0 %

Table (3.1) shows the study population's governmental institution representation to conduct, (70) questionnaires were distributed to an exploratory sample during July 2018 in order to examine the questionnaire validity and reliability. After ensuring the questionnaire validity and reliability, the researcher had distributed the questionnaire to the residual (70) employees of the population, where (54) Questionnaires were answered and returned. Thus, the total number of questionnaires subjected to the study and the statistical analysis in the next chapter is (54) questionnaires representing (77.14%) of the study population

Table (4.2) Research Population's Job Title Representation

Job Title	Frequency	Percent (%)
General Director	1	4.2 %
IT Manager	4	4.2 %
Engineer	26	32.8 %
Technician	27	28.5 %
Total	54	77 %

Table (3.2) shows the study population's job title representation. The statementrepresents an aspect of which the effectiveness of information

security policies should be measured. The questioner focused on knowing whether information security policies exist, implemented, monitored and constantly developed to face new challenges.

Measurement scale with response categories ranging from “strongly disagree” to “strongly agree”, which requires the respondents to indicate a degree of agreement or disagreement with each of a series of the statement related to the stimulus objects. The questioner was targeting the information technology department personnel, technicians, engineers and department heads, all are responsible for the security of the digital information of their company. Following are the findings of the questioner in each company, can see that most the percentages fluctuate between “Strongly agree” and “agree” which indicate the existence of a policy, but higher numbers answers with “agree” which indicate that the policies are ineffective either because it’s not properly implemented or not carefully monitored.

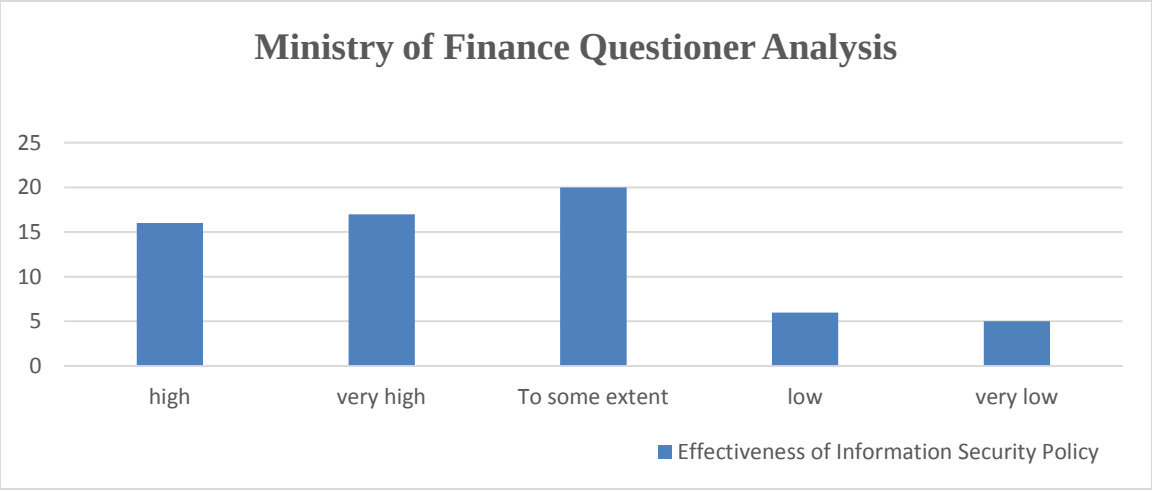

Figure (4.4): Results to the Ministry of Finance.

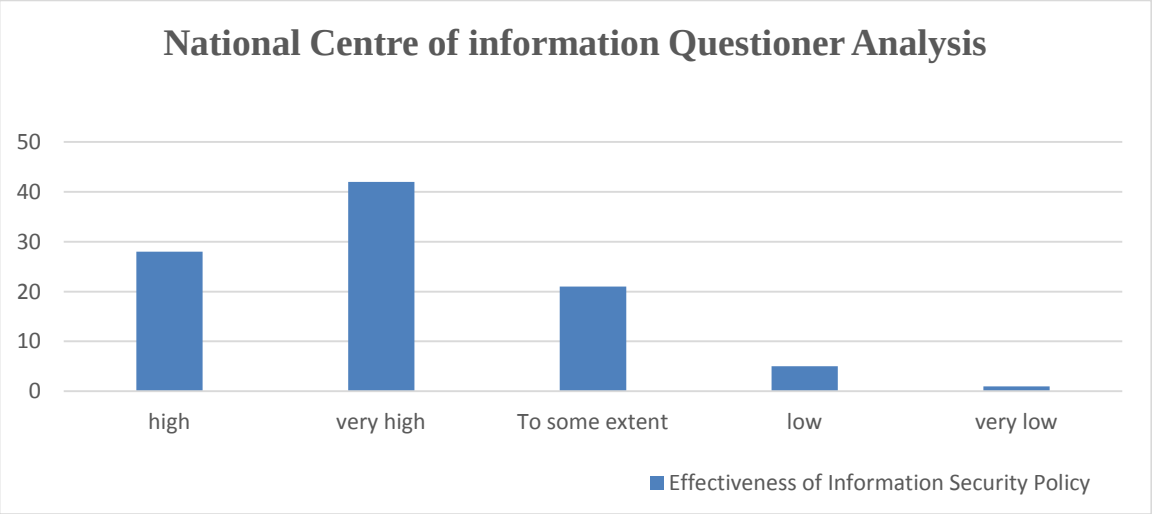

Figure (4.5): Results to National Centre of information

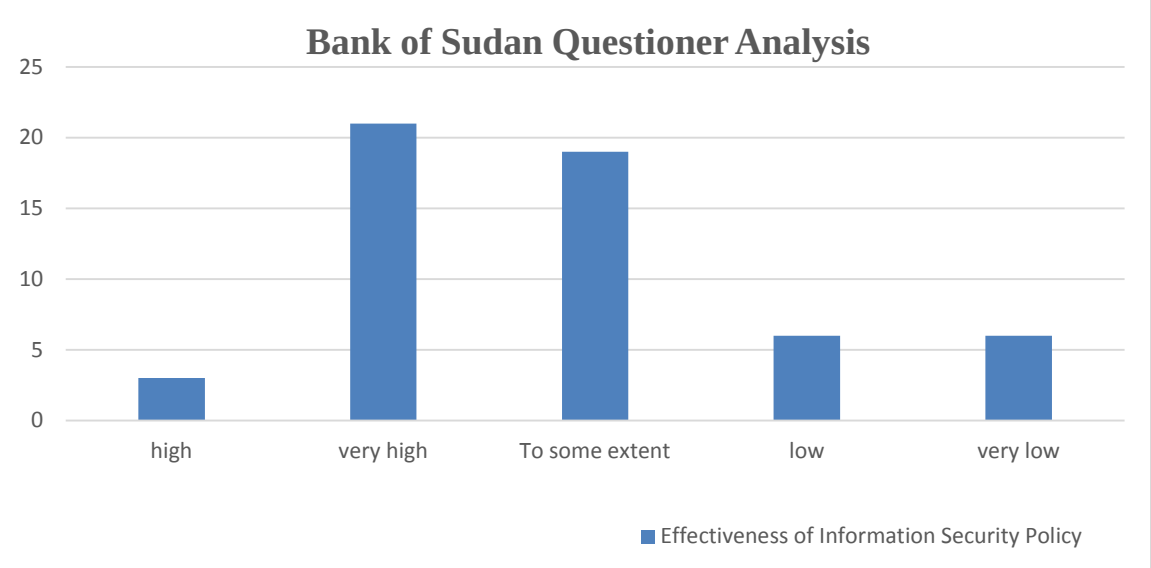

Figure (4.6): Results to Bank of Sudan.

4.7 Interviews Questions Analysis

An interview with the department heads was conducted for further investigation on some of the week points of the policies in place. The interview consisted of 13 questions, focusing on the monitoring and implementation of any exciting information security policy. Following is a brief summary of the interviews in each institute.

4.8 Ministry of Finance

The interview was with the IT manager in the ministry and in the course of further understanding the implemented policies and the regulations of information security policies, which are being followed, and to what extent it is believed that those regulations are being followed. And according to him the ministry doesn't follow a universal standard, rather a set of rules and regulations set by a group of experts in cooperation with the IT department, but facing the issue of getting the staff to obliged to those rules, and emphasized the fact that those regulations are not mandatory which makes monitoring and following those policies through very hard.

From the interview it was also understood that only one staff member has a professional certificate in information security, which makes following through with implementation of information security policy in the entire institute a very hard job that also led to the questions regarding the awareness of the importance of information security policies, and how only elective personal attended a training course regarding the issue, and how the awareness circle stopped there,there is also no budget for this particular subject, and management still not very involved in setting the security policies that help in achieving its goals, although there is an awareness of the importance of having an effective information security policy in place and it has been mentioned that the policies that have been in place since 2007 but only been reviewed

once since then, and the policy doesn't include risk and socio-technical contingencies, incidents regarding information security are handled internally and on a case by case basis following the country computer crime laws and civil services regulations.

There is an IT team, whose main responsibility is to raise the awareness amongst the staff regarding the importance of information security, but there is no official Written down documents regarding information security policies, nor there tool of managing the implementation process.

Finally, the interviewed manager feels that the main issue in the ministry is an awareness of the importance of having effective solid information security. Also, the interview, and coupling that with the fact that only 55% of the IT department staff actually answered the questioner it has been understood that the main problem in this institute is the awareness of the importance of information's security, awareness amongst management and staff.

4.9 National Center of Information

In this institute, the interviewed personal was the manager of network security; this company also does not have a universal standard security policy in place, the policy in place was developed by a team of experts in cooperation with the IT department and higher management. The policy focuses mainly on protecting physical network structure, access points and password management systems. Make sure all systems are up to date, but there is a password complexity issue. The manager estimates that only 40% follows the policies in place.

The interviewed manager expressed concerns that the policies of information security which has been set by his department being followed by employees, especially regarding password complexity.

The institution has 12 information security professionals involved in the information's security tasks, only one with a CEH1 certificate. Also,there is continues awareness programs – lectures, approach, portals and events in place – which eliminates awareness issues in this institute. Also, 70% of the budget is for information security policies implantation and review, and the management is involved in setting guidelines for the information security system to support the company's general goals, which include security, reliability and availability. Likewise, there are contingency guidelines regarding risks and socio-technical issues with respect to information security nonetheless incidents are handled on a case-by-case bases.

This institute has documented information security policies, authorized by top management; those policies are reviewed annually and adjusted to meet the latest technology development. Similarly, there are three different techniques to measure the effectiveness of information security policies; there are also regular questioners and perpetration testing besides the installed programs that digitally monitors the effectiveness of the information security policy.

At the end of the interview and coupling that with the fact that 20% of the IT department sample who answered the questioner believes that the information security policy in place is somewhat effective, leading to the belief that there is an implementation issue regarding the information security policies in this institute - employees failing to carry out instructions and not fully comprehend the importance of information security policies.

4.10 Bank of Sudan

In this institute, the department head of information security was interviewed, also a supervisor and an IT employee, all three confirm the existence of a documented information security policy, and it has been developed with cooperation between IT department, top managers and external experts.

The staff involved with the information security task has 9 information security professionals, three of whom has a CISP certificate and 6 have CEH certificates Open budget is designated and is only constricted by upper management approval, and the management is involved in setting strategies that fall in line with the general institute goals, management is also involved in approving any security objectives that are developed by the IT department.
All three also agreed that the information security policies are reviewed annually and adjusted to meet new technology developments, but the auditing of the implementation and effectiveness of the policies is done roughly every four times a year.

The institute has a critical incident response team that is responsible for evaluating and dealing with any incident that might occur regarding information security. The techniques in place to measure the effectiveness of information security policies included using official emails, regular discussions, reports and installed software for data collection and analysis. Thereare regular awareness programs portal forms, emails and practical presentations to involve employees in the information security issue.

All three of the interviewed personals agreed that the main issue that is facing the implementation of the information security policies is the employee's awareness of the importance of information security, and following throw the instructions regarding information security. The department head referred to the age of most employees as one of the reasons mentioning that older employees are less likely to follow instructions on technological matters.
At the end of the interview the minister and bank of Sudan seems to have the most effective information security system, and with the results of the questioner in mind it has been found that 97% of the IT department sample responded to the questioner, and 42% view the implemented system as highly effective, coupling that with the answers in the interviews there are mainly

implementation issues – employees failing to carry out instructions and not fully comprehend the importance of information security policies.

4.11 Recommended Solution

In this section, a code was applied to the server, which checks the policies applied to the network, whether it is implemented or not. For example, the firewall is responsible for the control of the package flow on the network, so the code was created To monitor Specific Firewall Rules which indicate its security& Send an SMS if those rules in the firewall were not properly applied. To tested this code through the server so used this code CHECK_STATUS=$(service iptables status).To check the firewall status found the firewall is not running then the system sends SMS alarm to the phone. Realize the command in this screenshot:

```
#############################################################################
 This Code To monitor Specific Firewall Rule is applied or not & Send SMS if it's not working
#######    OS : Redhat 6.5 ##################################################################################
#############################################################################

## CHECK FIREWALL STATUS
service iptablesstaus
#######################################################
#[root@test ~]# service iptables status
#iptables: Firewall is not running.
#############################################################
CHECK_STATUS=$(service iptables status)
if (( $CHECK_STATUS == "iptables: Firewall is not running." ))
then
$SEND_SMS 24922902760 "Firewall is not running"
if
#CHECK_IP TAPLES ACTIVE RULES
```

Then used this code #CHECK_IP TAPLES ACTIVE RULES to make checked for IPtables active rules in firewall after when status appear typed this code CHECK_STAT=$(iptables -L | grep -issh | awk '{print $12}') to check SSH rule for firewall founded status was drop to system sent the SMS alarm to the phone saw the result commend in this screenshot:

```
iptabels -L

################################ result of ABOVE command ####################
#-A INPUT -p tcp --dport 22 -m state --state NEW -j DROP    # Deny  SSH connections.
#-A INPUT -p tcp --dport 80 -m state --state NEW -j ACCEPT  #ALLOW HTTP
#-A INPUT -p tcp --dport 443 -m state --state NEW -j ACCEPT    #ALLOW HTTPS
##############################################################################
CHECK_STAT=$(iptables -L | grep -i ssh | awk '{print $12}')

if (( $CHECK_STAT == "DROP" ))
then
$SEND_SMS 24922902760 "XXX rule drop the connection from outside"
else
$SEND_SMS 24922902760 "XXX rule not drop the connection from outside, please check it"

################################################
# check number of bytes drooped in some rule
iptables -L -n -v
### OUTPUT WILL BE like THIS
#Chain INPUT (policy DROP 0 packets, 0 bytes)
#pkts bytes target     prot opt in     out     source           destination
#1000  2340  DROP       ssh  --  *      *       x.x.x.x            x.x.x.x

BYTES_DROOPED=$(iptables -L -n -v | grepssh  | awk '{print $2}')
$SEND_SMS 24922902760 "Bytes drop XXX rule is $BYTES_DROOPED "
```

4.12 Summary

To summarize this research finds that the main problem of the information security policies in the public sector in Sudan is the review, development and enforcement of a documented policy of each institution, accordingly the code was developed to help the monitor and regularly evaluate and develop the security policy of the institution.

Chapter Five
Conclusion and Recommendations

5.1 Conclusion

The research set out to assess the status of information security in the public sector in Sudan. More specifically the research was to evaluate the Effectiveness' of information security policy within the public sector setting; this was because found lack of information security governance framework, which has been, identified as one major factor affecting information security implementations. Several objectives in line with our research were identified, and its achievement or lack of it is discussed below. This chapter includes the most important conclusions, which have addressed the Effectiveness of information security policy in the public sector in Sudan. In addition, this chapter shows the proposed most important recommendations which may enhance the performance and to evaluate the effectiveness of information security policies and application of the public sector in Sudan. This research highlighted the need for an effective information security policy program within most organizations to be more effective. Examined and assessed the efficacy of information security policies and application at the public sector entities and came, and recommend solutions and guidelines to improve the development of the effectiveness of information security frameworks and practices at Sudanese public sector and that enhance the performance of the publicsector.

5.2 Recommendations

This section presents specific recommendations to the effectiveness of information security policies in the public sector in Sudan based on the findings discussed in the previous chapter. Following are the recommendations:

- Constantly manage and develop the policies in place, ensure the implementation and provide better awareness programs.
- The implementation of security policy should be reviewed independently on a regular basis.
- Sudan public institution should apply mechanisms to enable evaluating and controlling the kinds and costs of security incidents and the potential damage.
- There should be founded Information classification scheme or guideline in place; which assist in determining how the information is being handled and protected.
- Sudan public institutions should establish a formal reporting procedure or guideline for users, to report security weakness in, or threats to, systems or service
- The developed code in this research can be manipulated to include more than just the network; it should include all ICT equipment and all digital information in the institution.

References

[1]. P. J. Ortmeier, “Introduction to security: operations and management” Pearson Elsevier.com, 2017.

[2]. R. Ismail and A. Zainab, "Information systems security in special and public libraries: an assessment of status," arXiv preprint arXiv: 1301.5386, 2013.

[3]. M. Ula, Z. Ismail, and Z. M. Sidek, "A Framework for the governance of information security in banking system," Journal of Information Assurance & Cyber Security, vol. 2011, pp. 1-12, 2011.

[4]. N. S. Safa, R. Von Solms, and S. Furnell, "Information security policycompliance model in organizations," Computers & Security, vol. 56, pp. 70-82, 2016.

[5]. M. Alshaikh, S. B. Maynard, A. Ahmad, and S. Chang, "Information Security Policy: A Management Practice Perspective," arXiv preprint arXiv: 1606.00890, 2016.

[6]. K. AlGarni, Information Security Policy for E-government in Saudi Arabia: Effectiveness, Vulnerabilities and Threats: Rochester Institute of Technology, 2015

[7]. Principles of Information Security, 3rd Edition, Information security principle and practice by Mark Stamp.

[8]. R. Von Solms and J. Van Niekerk, "From information security to cybersecurity," computers & security, vol. 38, pp. 97-102, 2013.

[9]. T. P. Layton, Information Security: Design, implementation, measurement, and compliance: Auerbach Publications, 2016.

[10]. John Vacca “Security information management” Elsevier CPSC449 /FALL2014

[11]. M. Whitman and H. Mattord, Management of information security: Nelson Education, 2013.

[12]. J. Granneman, "IT security frameworks and standards: Choosing the right one," TechTarget, 2013.

[13]. J. REES, S. BANDYOPADHYAY, and E. H. SPAFFORD, "A Policy Framework for Information Security," 2014.

[14]. Khaled, (2015).Thesis. Information Security Policy for E-government in Saudi Arabia, Institute of Technology, Rochester,NY, May 14, 2015

[15]. W. A. Cram, J. G. Proud foot, and J. D'Arcy, "Organizational information security policies: a review and research framework," European Journal of Information Systems, vol. 26, pp. 605-641, 2017.

[16]. S. E. DeFranzo, "What's the difference between qualitative and quantitative research," Retrieved fromsnap survey. com, 2011.

[17]. S. Wyse, "What's the difference between qualitative and quantitative research," Retrieved, vol. 10, p. 2017, 2011.

[18]. N. M. Mbithi and M. ORWA, "An information security governance framework for the public sector in Kenya," University of Nairobi, Kenya, 2012.

[19]. PimSewuster, "Information security in practice (The practice of using ISO 27002 in the public sector", s4009126, Erik Poll,181 IK .2010.

[20]. I. Veseli, "Measuring the Effectiveness of Information Security Awareness Program," 2011.

[21]. I. Alsmadi, R. Burdwell, A. Aleroud, A. Wahbeh, M. A. Al-Qudah, and A. Al-Omari, "Introduction to Information Security," in Practical Information Security, ed: Springer, 2018, pp. 1-16.

[22]. C. Tikkinen-Piri, A. Rohunen, and J. Markkula, "EU General Data Protection Regulation: Changes and implications for personal data collecting companies," Computer Law & Security Review, 2017.

[23]. S. Bauer and E. W. Bernroider, "From information security awareness to reasoned compliant action: analyzing information security policy compliance in a large banking organization," ACM SIGMIS Database: the DATABASE for Advances in Information Systems, vol. 48, pp. 44-68, 2017.

[24]. D. H. A. Ibrahim, N. Musa, and C. K. Leng, "An Evaluation of Security Governance Model in Organizational Information Technology or Information Systems Security Implementation," Journal of Telecommunication, Electronic and Computer Engineering (JTEC), vol. 10, pp. 131-135, 2018.

[25]. G. D. Moody, M. Siponen, and S. Pahnila, "TOWARD A UNIFIED MODEL OF INFORMATION SECURITY POLICY COMPLIANCE," MIS Quarterly, vol. 42, 2018.

[26]. E. Amankwa, M. Loock, and E. Kritzinger, "Establishing information security policy compliance culture in organizations," Information & Computer Security, pp. 00-00, 2018.

[27]. T. R. Peltier, Information Security Policies, Procedures, and Standards: guidelines for effective information security management: Auerbach Publications, 2016.

[28]. T. P. Layton, Information Security: Design, implementation, measurement, and compliance: Auerbach Publications, 2016.

[29]. F. S. Pinheiro and W. R. Júnior, "Information security and ISO 27001," Journal of Management & Technology, vol. 3, 2016.

[30]. B. C. Stahl, N. F. Doherty, and M. Shaw, "Information security policies in the UK healthcare sector: a critical evaluation," Information Systems

Journal, vol. 22, pp. 77-94, 2012.

[31]. P. J. Ortmeier, Introduction to security: Pearson, 2017.

[32]. P. Lund, "Information Security Awareness amongst students: A study about information security awareness at universities," ed, 2018.

[33]. K. A. Alshare, P. L. Lane, and M. R. Lane, "Information security policy compliance: a higher education case study," Information & Computer Security, vol. 26, pp. 91-108, 2018.

[34]. M. M. Ratchford, "BYOD: A Security Policy Evaluation Model," in Information Technology-New Generations, ed: Springer, 2018, pp. 215-220.

[35]. S. V. Flowerday and T. Tuyikeze, "Information security policy development and implementation: The what, how and who," computers & security, vol. 61, pp. 169-183, 2016.

[36]. A. Da Veiga and J. H. Eloff, "A framework and assessment instrument for information security culture," Computers & Security, vol. 29, pp. 196-207, 2010.

[37]. S. Mishra and L. Chasalow, "Information security effectiveness: A research framework," Issues in Information Systems, vol. 12, pp. 246-255, 2011.

[38]. Y. Han, J. Chan, T. Alpcan, and C. Leckie, "Using virtual machine allocation policies to defend against co-resident attacks in cloud computing," IEEE Transactions on Dependable and Secure Computing, vol. 14, pp. 95-108, 2017.

[39]. P. M. Tehrani, J. S. B. H. Sabaruddin, and D. A. Ramanathan, "Cross-border data transfer: Complexity of adequate protection and its exceptions," Computer Law & Security Review, 2018.

[40]. A. Dobrovoljc, D. Trček, and B. Likar, "Predicting Exploitations of Information Systems Vulnerabilities Through Attackers' Characteristics," IEEE Access, 2017.

[41]. A. Dobrovoljc, D. Trček, and B. Likar, "Predicting Exploitations of Information Systems Vulnerabilities Through Attackers' Characteristics," IEEE Access, 2017.