INFORMATION SECURITY STANDARDS AND POLICIES COMPLIANCE BY NIGERIAN BANKS

By

Williams Adedayo Solomon

216069213

A thesis submitted in fulfilment of the requirements for the degree of Doctor of Philosophy

School of Management, IT and Governance
College of Law and Management Studies

Supervisor: Professor Manoj Maharaj

2019

DECLARATION

I, Williams Adedayo Solomon, affirm as follows:

a) The research report presented in this thesis, represents my own original work except where otherwise specified.

b) This work has not been presented for any degree or examination at any other university.

c) This thesis contains no other persons' data, pictures, graphs or other information, unless specifically admitted as being sourced from such.

d) Equally, the work does not contain other scholars' writings, unless explicitly acknowledged as being sourced from them. Where other written sources have been quoted, then:

   i. Their contents have been thoroughly paraphrased, while the ideas sourced from them have been accordingly referenced;

   ii. Where they have been quoted *verbatim et literatim,* their writing has been properly located within inverted commas and duly referenced.

   iii. In any section I have reproduced a publication of which I am author, co-author or editor, I have specified in detail which part of the publication was written by me alone and have fully referenced such publications accordingly.

This research work does not reflect texts, graphics or tables copied from the Internet, unless acknowledged as expected, and the source being detailed in the thesis and in the References Section.

Signature: 

Date: 21st April , 2021

DEDICATION

This thesis is dedicated to God, my family and my late parents.

ACKNOWLEDGEMENTS

The completion of this PhD study would not have been possible if some special people hadn't believed in me. While stressful, it was an interesting and unforgettable experience that enhanced my personal development. It is not about how knowledgeable I am, but about the Almighty God who stood by me through it all. I therefore say a big THANK YOU to Him.

I would like to thank my supervisor, Professor Maharaj Manoj, for the interest he showed in this study, his academic expertise and unconditional support and his patience and perseverance. His mode of supervision boosted my confidence and self-reliance.

My thanks to the University of KwaZulu-Natal's Ethical Committee for useful guidance. I appreciate all my friends and colleagues who supported me both financially and academically as well as Dr Ojuregbe, Dr Atiku, Mr Ola, Miss Ofusori and all the member of Deeper Life Campus Fellowship.

My siblings, particularly Dr. Opeyemi Williams and Mr Olakitan Williams offered on-going encouragement and financial assistance which was much appreciated. A big thank you to my brother, pastor and daddy, Dr. Adeyeye Olufemi for your encouragement and financial assistance throughout my journey and as well as Pastor Odewale and his wife. Also to my daughters Giwa Fiyinfoluwa Oladuntan, Taiwo and Toyin a big thank to you all.

Finally, special thanks to my wife Odunayo Williams and my sons Toluwanimi Daniel, Temiloluwa David, and Toluwalase Dan Williams for understanding when I could not spend quality time with them.

ABSTRACT

The modern banking sector is highly dependent on customer information to carry out its daily business. Such information is thus an asset which must be protected from threats; hence banks have adopted policies and standards in this regard. The Nigerian banking sector is characterised by on-going information security breaches. The reasons include low levels of individual and corporate compliance with information security standards and policies and procedures (ISSsPs), as well as the fact that banks focus on data usage optimisation rather than the privacy and security of customer information.

This study examined the extent to which Nigerian bank employees comply with information security standards and policies and whether or not a relationship exists between the level of compliance and information security breaches. The theories of planned behaviour, protection motivation and self-efficacy were employed to identify the factors that motivate such compliance. The results show that all the motivational factors influence employee behavioural intention (EBI) to comply with ISSsPs. In the same vein, employee behavioural intention was found to influence such standards and policies.

Hypotheses were also developed to investigate the mediating effect of EBI on the relationship between motivational factors and ISSsPs. The analysis showed that EBI has a partial mediation effect on the relationship between motivational factors and compliance with ISSsPs.

The analysis of the effect of the motivational factors on ISSsPs revealed that the perceived severity of a penalty has a significant influence on compliance with ISSsPs. Certainty of detection was then regressed on employee intention to comply with ISSsPs and the results show that it has a significant effect. Furthermore, it was established that normative beliefs, the perceived effectiveness of information security standards, an awareness of information security threats, and perceived bias have a positive influence on an employee's intention to comply with ISSsPs.

The study also investigated the relationship between the compliance rate and experience of information security breaches. The analysis showed that there is a positive relationship between banks reviewing their ISSsPs and their experience of information security breaches. Thus, the more banks experience information security breaches, the more they review their standards. It was found that Nigerian banks review their information security codes and standards at least once a year.

Finally, the study proposes and validated an employees' compliance framework that has the potential to significantly improve employees' compliance with ISSsPs, thus mitigating the effects of information security threats on Nigerian banks.

DERIVED PUBLICATIONS

1. **Williams, A.S.,** Maharaj, M.S. and Ojo, A.I. (2019). Employee Behavioural Factors and Information Security Standard Compliance in Nigerian Banks. *International Journal of Computing and Digital Systems, 8*(4), 387-396.

2. **Williams, A.S.** and Maharaj, M.S. (2021). Factors Influencing Information Security Standards and Policies Compliance by Nigeria Banks. *The Africa Journal of information systems (Accepted)*

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

Abbreviation	Full Word
ATM	Automated Teller Machine
BS	British Standards
BSI	British Standard Institution
CBN	Central Bank of Nigeria
CCTV	Close Circuit Television
CIOs	Chief Information Officers
COBIT	Control Objectives for Information and Related Technologies
COD	Certainty of Detection
DMBs	Deposit Money Banks
EBI	Employees Behavioural Intention
EFCC	Economic and Financial Crimes Commission
EPHI	Electronics Protected Health Information
FBI	Federal Bureau of Investigation
FFIEC	Federal Financial Institutions Examination Council
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
GLBA	Gramm Leach Bailey Act
HIPAA	Health Insurance Portability and Accountability Act
IDS	Intrusion Detection System
ICICI	Industrial Credit and Investment Corporation of India
ICT	Information and Communication Technology
IFG	Integrity Financial Group
IP	Internet Protocol
ISA	Information Security Awareness
ISB	Information Security Breaches
ISO	International Standard Organisation
IS	Information Security
ISP	Information System Protocol
ISSsPs	Information Security Standards and Policies
IDs	Intrusion Detections
IT	Information Technology
NBS/EFCC	Nigerian National Bureau of Statistics/Economics and Financial Crimes Commission
MCAR	Missing Completely at Random
NCWG	The Nigerian Cybercrime Working Group
NEFF	The Nigeria Electronic Fraud Forum
NIBSS	Nigeria Inter-Banks Settlement Systems Plc
NIST SPs	National Institute of Standards and Technology/Special Publications
NITDA	National Information Technology Development Agency
NOB	Normative Belief
PEF	Perceived Effectiveness
PCI/DSS	Payment Card Industry/Data Security Standard
PCB	Perceived Compliance Behaviour

PIN	Personal Identification Number
PMT	Protection Motivation Theory
RFID	Radio - Frequency Identification
RMF	Risk Management Framework
SD	Standard Deviation
SPSS	Statistical Package for Social Sciences
STA	Security Standard Awareness
SOP	Severity of Penalty
SOX	Sarbanes – Oxley Act
TPB	Theory of Planned Behaviour
TAC	Transaction Access Code
US	United States of America
VIF	Variance Inflation Factor

CHAPTER ONE
INTRODUCTION

1.1 Introduction

The Nigerian banking sector is characterised by information security issues such as cyber-attacks, data theft and internet fraud (Jegede, 2014; Ibikunle and Eweniyi, 2013; Wada and Odulaja, 2012). Studies suggest that a low level of compliance with Information Security Standards (ISS) is one of the major causes of this situation (Deloitte, 2015). This is arguably so because, as in many organisations, the speed and capacity of data usage optimisation is prioritised over security and privacy (McGuire and Dowling, 2013; Van and Allan, 2013). Policies and standards for information security provide organisations with accurate security information and a strong security defence. In the medium to long term, this enables improved data usage, prevents theft and increases customers' confidence (Deloitte, 2015; McGuire and Dowling, 2013).

This study is concerned with users' involvement in Information Security Standards and Policies (ISSsPs) compliance, precisely bank employees as users. Despite its importance, such involvement has received little attention in the Nigerian security compliance literature (Herath *et al*., 2014; Peterson, 2014). The study thus explores banking employees' behavioural understanding of information security compliance. It proposes a conceptual framework to understand the behavioural factors that influence employee intention to comply with ISSsPs. It is anticipated that this will assist banks to achieve improved compliance and thus significantly reduce instances of data privacy breaches, cyber theft and internet fraud.

1.2 Background to the Study

The rapid evolution of information and communication technology (ICT) has had a significant impact on countries around the world, including Africa, where it is still in its emergent stage (Kayisire and Wei, 2015). However, ICT plays a significant role in almost all spheres and domains of human endeavour. Ellis (2019) asserts that these domains are witnessing a paradigm shift from the use of primitive tools to technology-powered ones. The impacts have been both positive and negative, including exposure to information security threats such as data privacy and confidentiality breaches; cyber-attacks and theft; and cyber monetary fraud, amongst others (Nyawanga, 2015).

Banks act as financial intermediaries and provide secure payment platforms to support the national economy, assisting in implementing monetary policies. Consequently, this exposes them to cyber threat vulnerabilities. Like banks around the world, Nigerian banks need to manage customers' finance, ensure the privacy of their data and generally contribute to the security of the business environment for citizens, investors and businesses (Wada and Odulaja, 2012). Gashi and Peci (2020) postulate that, indeed, a secure banking environment is a national image maker. However, Nigerian banks' record in protecting customers' accounts and safeguarding their data privacy has been worrisome (Nyawanga, 2015; Wada and Odulaja, 2012).

Online identity theft through phishing, data interference, forgery, spamming and electronic fraud are examples of the cyber threats recorded by Nigerian banks (NIBSS, 2015). Moreover, Akinbowale *et al.* (2020) asserted that internet crime reports placed Nigeria in third position in terms of online global financial crime, while Nawaya *et al*. (2019) saw Nigeria as one of the leaders when it comes to cases of Automated Teller Machine (ATM) fraud. The Nigeria Electronic Fraud Forum (NEFF) reported a loss of N203 billion by Nigeria's Deposit Money Banks (DMBs) due to cases of cyber fraud (Akinbowale *et al*., 2020). According to a Nigerian inter-bank settlement system report, the country's banks lost N159 billion between the year 2000 and the first quarter of 2013 and N40 billion from January 2013 to September 2014 (Orji, 2019) to cybercrime. Cyber financial fraud has affected banking performance, resulting in insolvency and bankruptcy, thereby cntributing significantly to the country's weak capital market and low credit rating (Ajayi, 2019; Sunday and Bamidele, 2014). Theoretical and practical approaches are thus required to decisively address cyber fraud amongst Nigerian banks and to mitigate its effects on the country's financial sector.

This study investigated the extent of Nigerian bank employees' compliance with ISSsPs, as well as the role played by motivational factors in employee intention to comply with standard information security policies and codes. ISSsPs codes are globally designed terms and mechanisms aimed at ensuring information security (PCI Security Standard Council, 2014). The Global Banking Forum, of which the Central Bank of Nigeria (CBN) is a member, has adopted a myriad rules and standards, namely the Federal Information Security Management Act (FISMA), Health Insurance Portability and Accountability Act (HIPAA), Sarbanes – Oxley Act (SOX), International Standard Organisation (ISO/IEC 17799) and Gramm Leach

Bailey Act (GLBA), among others (Akamai, 2015). This study aimed to establish the extent of individual Nigerian banks' compliance rates and attempted to investigate the relationship between the compliance rate and experiences of information security breaches, as well as the role of employee motivational factors in encouraging/ensuring compliance with ISSsPs.

1.3 Problem Statement

The increase in the number of cases of cyber fraud experienced by Nigerian banks has been recorded by Fadare (2015), Sunday and Bamidele (2014), Jegede (2014), Quarshie (2014), Olusola *et al*. (2013) and Wada and Odulaja (2012), amongst others. These studies focused on the adoption of ICT to combat cyber fraud (Fadare, 2015); a sociological perspective on the youth's involvement in cyber fraud (Jegede, 2014); the negative effect of financial crime on banking performance and the Nigerian economy (Sunday and Bamidele, 2014); and the role of law and the criminal code in preventing cyber theft (Olusola *et al*., 2013). Others highlighted the importance of information security compliance in preventing cyber fraud (Huntsman, 2015; Neghina and Scarlat, 2013). However, none of these studies investigated the extent of Nigerian banks' compliance with ISSsPs and its role in preventing cyber fraud.

Theoretical studies have also examined employees' motivational factors, otherwise known as behavioural factors, in order to evaluate their intention to comply with ISS codes and improve organisational compliance (Chiu and Tan, 2020; Herath *et al.,* 2014; Peterson, 2014). The impact of these factors on Nigerian banks' employee's compliance with international information security codes and standards has not been investigated.

The research problem investigated in this study was broken down into four sub-problems for proper contextualisation and measurability. These are explained in Sections 1.3.1, 1.3.2. 1.3.3 and 1.3.4.

1.3.1 First Sub-Problem

The extent of Nigerian banks' compliance with ISSsPs has not been empirically assessed, even though this is important in combatting cybercrime. Notably, Brunner Anderson (2020) observed that compliance with ISSsPs provides organisations with an effective information security tool and strengthens their security mechanisms. Furthermore, Anderson *et al*. (2012) identified the following advantages of complying with ISSsPs:

a) Identify potential vulnerabilities;
b) Objectively measure security issues;
c) Establish a priority list for compliance; and
d) Create information security awareness.

Nigerian banks are lagging behind in complying with ISSsPs in order to prevent cyber fraud (BSI, 2015). While a 2014 CBN report notes that the apex bank is praised for complying with ISO/IEC ISO/IEC 27001, the same cannot be said of mainstream Nigerian commercial banks, or for other international standards like FISMA, HIPAA, SOX, ISO/IEC 17799 and GLBA. This study thus aimed to identify individual Nigerian banks' compliance rates.

1.3.2 Second Sub-Problem

There is little empirical evidence to validate the hypothetical claims (Ibikunle and Eweniyi, 2013) that compliance with international ISSsPs reduces cyber theft. It is therefore important to empirically investigate the relationship between Nigerian banks' compliance rates and the experience of information security breaches. Given their widespread experience of cyber fraud and the few reported cases of international ISSsPs compliance, coupled with the lack of scholarly conclusions based on hard data, there is a need to determine if there is a relationship between the compliance rate and experience of information security breaches.

1.3.3 Third Sub-Problem

Employees play a significant role in enhancing organisational efficiency, that is, organisational compliance with international ISSsPs (Herath *et al*., 2014; Peterson, 2014). Investigations into the intrinsic and extrinsic motivational factors that contribute to employee intention to comply have not covered all possible factors, nor has a thorough examination been conducted on the theoretical underpinnings of these factors. This study sought to bridge this gap by incorporating awareness, perception biases, effectiveness of information security standard and policies compliance, normative belief, severity of penalty and certainty of detection as factors of interest.

1.3.4 Fourth Sub-Problem

No study has developed a framework that combines information security standards and policy compliance to show the dynamics of employee willingness to comply, particularly in the financial sector.

1.4 Research Questions

The following research questions emerged from the problem and sub-problems:

- What is the Nigerian banks' rate of compliance with international information security standards and policies?
- Is there any relationship between the compliance rate and experiences of perceived information security breaches?
- How do employee motivational factors contribute to their intention to comply with international information security codes and standards?
- What employee compliance framework highlights the compliance behaviour of employees in Nigerian banks?

1.5 Research Objectives

The following research objectives also arose from the problem and sub-problems:

- To examine the rate and extent to which Nigerian banks have complied with international information security standards and policies;
- To determine the relationship between the compliance rate and experiences of perceived information security breaches;
- To investigate the employee motivational factors that contribute to bank employees' intention to comply with international information security codes and standards; and
- To propose an employee compliance framework that highlights the compliance behaviour of employees in the Nigerian banking sector.

1.6 Justification for the Study

The justification for this study can be approached from a theoretical as well as a practical perspective. In practical terms, the importance of this study hinges on the fact that it proposes a working framework that employs non-technical means to secure Nigerian banks' information repositories and mitigate cyber fraud and theft. The non-technical means understands employees' behavioural factors towards organisational compliance with ISSsPs. From a theoretical perspective, the study offers a novel understanding of behavioural change in respect of ISSsPs compliance amongst Nigerian banks using the theory of planned behaviour, self-efficacy theory and protection motivation theory.

The study thus fills a gap in the body of knowledge on the utilisation of non-technical methods in general, and more specifically employee behavioural factors, in securing banks' information repositories.

1.7 Significance of the Study

The study's findings will benefit all stakeholders in the banking sector, as well as information security professionals. It presents the leadership of the banking industry with a behavioural framework that highlights their employees' behavioural dynamics and how these influences their compliance with ISSsPs. It will also support the banks' ISSsPs compliance framework and offer information security professionals a non-technical approach to mitigate information security threats, cyber fraud and theft.

1.8 Research Design

Creswell (2013) gave a precise explanation of research design as a continuous evolution from plans through data collection to data analysis. There are three main research design categories, which are exploratory, explanatory and descriptive. An exploratory research design, according to Sekaran and Bougie (2009), investigates the current environment to find new insights into an identified problem. Descriptive research extends and expands on exploratory research (Saunders *et al*., 2015), which also describes the phenomena or variables of interest. The exploratory research design on the other hand is used to expand on discussions, while explanatory research forms associations between constructs (Creswell, 2013). This study employs a quantitative research method. In relation to Smith *et al*. (2012), it was stated that a quantitative research design can validate a study's conclusions by verifying the established concepts and proving or disproving a proposed concept.

This study kick-started by critically reviewing related past studies to identify, conceptualise and operationalize employees' behavioural constructs that can influence employees' intention to comply, as well as their eventual compliance with ISSsPs. Secondly, using the theoretical underpinnings of the TPB, PMT and self-efficacy theory, and based on related past studies, a survey instrument was designed and administered to a sample of Nigerian bank employees. Thirdly, the data collected was analysed using appropriate statistical techniques and tools to provide answers to the research questions. Data cleansing was undertaken during the data

analysis process in order to achieve validity and reliability. Further details are provided in Chapter Four of this thesis.

1.9 Structure of the Thesis

Chapter One: Chapter One sets out the rationale for conducting the research. It highlights the increase in the number of cases of cyber fraud amongst Nigerian banks, which negatively impacts the banking sector and the economy. No previous studies have explored the extent of Nigerian banks' compliance with ISSsPs and its role in preventing cyber fraud. The chapter also notes that there is a lack of comprehensive information on employees' motivational factors, otherwise known as behavioural factors, in relation to their intention to comply with ISSsPs codes and improve organisational compliance. Consequent to these identified problems, the chapter contains drafted objectives to be achieved in this study and the related research questions.

Chapter Two: The second chapter reviews literature on the cybercrimes committed in and outside the banking sector both from an international perspective and in Nigeria. The effects of cybercrime and solutions highlighted in the literature are also discussed. The chapter presents a detailed review of information security breaches in the Nigerian banking sector, while information security standards governance amongst Nigerian banks are also emphasised. Moreover, the chapter encompasses the international standards and policies Nigerian banks subscribe to, with comprehensively details.

Chapter Three: Chapter Three discusses the theories that underpin this research. Seven theories that relate to individual expected behaviour towards certain actions are reviewed. The theories of planned behaviour, protection motivation and self-efficacy were selected because they are frequently referenced in studies on employees' compliance with ISSsPs and they comprehensively address the constructs used in this study. Other theories reviewed include the social cognitive, locus of control, social bonding and agent paradigm theories. The basic reasons for these theories not being used are explained, while a justification for applying the theories of planned behaviour, protection motivation and self-efficacy in the study are explained. In the same vein, the conceptualisation of the motivational aspects and their explanations were detailed in this chapter.

Chapter Four: Chapter Four discusses the research design, which outlines the process adopted to achieve the research objectives and answer the research questions. It presents the methodological framework which highlights the connection between the theories, research constructs, research objectives and research method employed to achieve the research goal. The survey instrument design, sampling methods and data collection and analysis are also discussed.

Chapter Five: The fifth presents the results of the data analysis conducted using the Statistical Package for the Social Sciences (SPSS). It begins with a description of the data in the form of a preliminary analysis, followed by the respondents' demographic characteristics. The various constructs are then presented and the fundamental assumption of regression analysis prior to the test of the hypothesised relationships is discussed. In the same vein, this chapter also detailed the exploratory factor analysis conducted to extract the significant factors for model development.

Chapter Six: Chapter Six discusses the study's findings. The discussion was based on the results generated from the analysis of the data collected. The discussion was done through the lens of objectives and hypotheses to provide answers to the research questions.

Chapter Seven: This chapter contains an employee compliance model along with the explanation on how individual motivational factors relate to the employees' behavioural intention and how the employees' behavioural intention in turn influences the actual compliance. Furthermore, the chapter equally contains the analysis of the data collected to validate the developed model. The comprehensive model for employee compliance was developed, where all the motivational factors are brought together. Finally, the details of the components and how they relate together are also discussed.

Chapter Eight: The study's theoretical, methodological and practical contributions are highlighted in this final chapter. In addition, the recapitulation of the objectives is carried out with the details of the evaluation of the model outcome. The chapter ends with a discussion on the study's limitations and makes recommendations for future research.

1.10 Chapter Summary

This chapter introduced the study by presenting the background to the myriad challenges posed by the evolution and adoption of ICT in the banking industry, especially in relation to the management and security of ever-increasing customer data. It outlined the problem statement that raises the specific theoretical and practical issues addressed. The chapter also presented the research questions and objectives, the justification for the study and its significance. A brief discussion of the research design was also provided. The structure of the thesis was also highlighted.

Chapter Two reviews the literature relevant to this study.

CHAPTER TWO
LITERATURE REVIEW

2.1 Introduction

This second chapter presents details on organisational information security challenges. It examines banking services, cybercrime and information security breaches in the banking sector, as well as the losses incurred. In addition, the causes and possible solutions to avert thse information security breaches are also detailed.

2.2 Organisational Information Security Challenges

Protecting information systems in an organisation is becoming a herculean task. While many organisations have adopted technologies to secure their information, technology alone cannot adequately safeguard their information assets from threats. Thus, end-user involvement is very important. Ali (2019) identified the various ways in which cybercrime can affect the banking sector, including identity theft, phishing, denial of services, malware, hacking, social engineering, automated online banking fraud, mobile phones and other electronic gadgets, social networks and electronic media platforms.

Bank management is thus called upon to address cybercrime (Spulbar and Birau, 2020). In the same vein, Ali (2019) drew attention to the need to develop awareness amongst employees in the banking and financial sectors, while the investigations of Akinyomi (2012) into the causes of fraudulent behaviour in the Nigerian banking sector concluded that greed was the foremost cause, as some employees considered their salaries to be sufficient. This study focuses on cybercrime as the major challenge confronting banks.

MK and Ramayah (2019) investigated the various security threats confronting banking institutions in Bangladesh. The study concluded that the Bangladeshi banking sector suffers from vulnerability to information security threats, which is exacerbated by the fact that banks depend wholly on Information Technology (IT) platforms in their daily transactions. Guobin and Lin (2015) noted that big data is vulnerable to threats due to the collection and storage methods employed and the numerous links to it.

The challenge of information insecurity in banking institutions calls for ISSsPs, information management, risk management and disaster recovery. However, ISSsPs ensures the security of

organisational assets and provides a means to ensure the availability, confidentiality and integrity of such assets (Clark *et al*., 2020). Equally, Wei *et al*. (2020) investigated the relationship between risk factors and potential vulnerability within the banking system and concluded that information security should be a priority. They also concluded that IT is essential in this quest.

Wei *et al*. (2020) observed that information is a fundamental organisational asset, hence it is imperative to protect it from intruders. Information is the life force of companies, since the daily activities and duties of employees and employers depend on it. Organisations thus have to protect their assets and information while coping with the changing technological environment. Assets could take the form of traditional documents, text messages, video, email, audio, RFID, and so on, using different systems and technologies like databases, documents, records, content management systems, social networking tools and mash-ups, with many of these hosted externally using technologies like cloud computing (Mishra *et al*., 2020). However, securing such information calls for careful management as it is prone to attack by cybercriminals.

While antivirus and patch management software reduce the stress on users, the accurate application of computer network resources and appropriate use of passwords cannot be managed by technology but must be enforced through organisational policies (A Chronology of Data Breaches). Relying solely on technological solutions to reduce information security risks is pointless, as Kai (2020) highlighted in studies that investigated thirteen notifications pertaining to data security breaches by state and federal employees. The results show that some of the notifications convey negative messages. However, the author added that the template is useful in informing the user of the requirements of the law and could assist in educating employees on information security threats. Section 2.3 below examines the information security challenges confronting Nigerian banks.

2.3 Cybercrime and Information Security Breaches in the Banking Sector

In 2016, the Federal Bureau of Investigation (FBI) Internet Crime Complaint Centre recorded 1,408,849 reported losses amounting to a total of $4.63 billion (Smith, 2017). Older people over the age of 60 suffered the most, with 55,043 cases and a total loss of $339,474,918. The

top-ranked cybercrime in 2016 was business email compromise/email account compromise (BEC/EAC) with a total loss of $360,513,961. This was followed by identity theft, credit card fraud and phishing and hacking at $58,917,398, $48,187,993, $31,679,451 and $55,500 respectively (Smith, 2017 cited in Chevers 2019).

Cybercrime in Nigeria commenced in the 1990s and has continued to increase and spread its tentacles to various organisations. Governmental and non-governmental organisations, the public sector and non-profit organisations have launched initiatives to combat this scourge (Mierzwa and Scott, 2017). The study by Zajko (2018) on cybercrime focused on securing government and military information security systems. The author also examined the vulnerability of infrastructure within the context of policy plans put in place by the US. In addition, Atiku and Fields (2017) critically examined the emergence of cyber threats from a technical perspective, focusing on the role of law enforcement agencies in apprehending and prosecuting offenders. He found that there is constant violation of the laws adopted to prevent information breaches, with several cases of information crimes handled by law enforcement each year. Thakkar *et al*. (2020) developed a comprehensive framework to understand cyber threats, taking into account the strategy development process. They grouped information security threats into four categories, namely attacks on mail, spam-associated threats, malware and phishing. Organisations remain vulnerable to threats if appropriate precautions are not taken. Malik and Islam (2019) examined the effect of cybercrime in the banking industry. The study concluded that information security awareness is crucial in addressing cybercrime and enhancing organisational performance. It also considered the moderating influence of information security awareness in the banking industry and found that while cybercrime has a negative influence on organisational performance, information security awareness reduced this influence.

Cybercrime's effect on banking development and business growth must thus be addressed by management. Ali (2019) as well as Ojeniyi and Abdulhamid (2019) raised the issue of the need to develop awareness amongst employees in the banking and financial sectors in order to ensure a sustainable business environment. Miller (2014) notes that information security breaches have resulted in the loss of millions of dollars and sabotaged organisational operations. The author argues that this is due to the fact that IT security controls are low in light of the severity of information security threats.

Cybercrime and information breaches are the major problems confronting African banking institutions, especially in Nigeria, with negative economic consequences. The most common cybercrimes in Nigeria are theft and fraud (constituting 75% of cybercrimes), which are very common amongst the youth (Nigerian National Bureau of Statistics/Economics and Financial Crimes Commission, 2009). Cybercrime can be defined as any type of misdemeanour in cyberspace and refers to a particular way of using the internet (Hassan *et al*., 2012). It emerged in the 1960s in the form of hacking, the distribution of illegal materials, trespassing and the tapping of telephone calls. During the 1980s, there was an alarming rise in the spread of computer viruses (Olufunke, 2010). The development and adoption of ICT paved the way for further cybercriminal activities and added to the list of criminal activities in cyberspace. Today, the internet is used to commit transactional crimes, especially with e-banking currently gaining ground in Nigeria and other parts of Africa.

Bank customers and online buyers battle with the unknown risk of their information falling into the hands of hackers and criminals. The lack of regulations and standards dealing specifically with card-related crime, particularly in Nigeria, may provide criminals with a loophole to freely perpetrate their acts. The police currently treat card-related crimes like other fraudulent acts. This study explored different classes of cybercrimes which have both direct and indirect effects on the Nigerian financial system. Kayode *et al*. (2016) listed common ICT threats,such as phishing, electronic spam emails, identity theft, cyber-stalking and other activities that are peculiar to Nigeria. In the same vein, Alese *et al*. (2014) developed a framework which ascribes the major sources of cyber threats to micro-finance institutions in Nigeria, as well as information security policies. The authors also examined the modern challenges posed by cybercrime; the channels through which such crimes occur; existing mechanisms to curb the trend; the efficiency of information security; the possibility of modern techniques tackling cybercrime; and the role of government in reducing cyber threats.

2.4 Cybercrime Experiences amongst Nigerian Banks

Cybercrime can be defined as misdemeanours in cyber space. It involves the criminal use of the internet or the unlawful use of ICT devices. Cybercrime has escalated to the point where it now threatens the national security of many countries, including Nigeria, and even affects those that have adopted sophisticated technologies, such as the US (Hassan *et al*., 2012). Nigeria has been ranked 43rd in Europe, the Middle East and Africa and third among the ten nations with

the highest rate of cybercrime in the world (Frank and Odunayo, 2013). The Nigerian Cybercrime Working Group (NCWG) was created to meet the objectives of the NCI, but its efforts have not kept pace with the growth of cybercrime. The intensity of cybercrime in Nigeria has had significant consequences for banking sector performance and national productivity. The scope and level of cybercrime in the banking sector is not surprising, given Nigeria's profile as a corrupt and fraudulent nation as a result of the insatiable appetite for profit. The scale of fraud has increased and banks are losing billions of Naira. Cybercrime has resulted in widespread distress and socio-economic suffering. It also has a detrimental effect on industrial growth, as many banks have succumbed to bankruptcy. Saulawa and Abubakar (2014) highlight financial losses and economic downgrading as a result of cybercrime. Indeed, it has led to the demise of 36 Nigerian banks (Kida and Goyal, 2018). In addition, Onyesolu and Ezeani (2012) classified Nigerian cybercrime experiences into two major categories: Automated Teller Machine-Personal Identification Number (ATM-PIN) crimes and cyber theft.

2.4.1 ATM-PIN Cybercrime

ATM-PIN cybercrime is one of the leading cybercrimes in Nigeria. The main method is PIN theft, which is achieved through skimming, shoulder surfing, cameras, key pad recording, etc. Criminals use different card trapping devices, including slim mechanical tools sometimes encased in plastic transparent film, which are placed in the card reader slot. Hooks are then attached to the probes, preventing the card from being returned to the customer when the transaction is complete. When the user expresses concern, the criminal offers support, suggesting that they re-enter the PIN. By watching closely, the criminal is then able to access the PIN (Onyesolu and Ezeani, 2012).

Once the customer leaves the ATM, believing that their card has been retained, the criminal uses a probe to extract the card. Having accessed the PIN, he/she can withdraw money from the account. However, shoulder surfing, another means of ATM-PIN theft, is referred to as direct observation as the criminal observes the number the person inputs on the keypad. The criminal places him or herself in a strategic position, but not in direct proximity to the ATM. He/she watches as the user inputs their PIN. Some criminals install miniature video cameras that are easily obtained close to the PIN pad to record the PIN details.

Cybercriminals also place fake PIN pads over the authentic ones. The overlay captures the PIN data and stores the information in its memory. The fake PIN pad is then removed, and recorded PINs are downloaded. Fake PIN pads can be almost identical in appearance and size to the original. An additional type of overlay that is more difficult to detect is a 'thin' one that is transparent, used in conjunction with card data theft. This provides the criminal with the information required to access an unsuspecting customer's account.

Criminals also use skimming to obtain card data. "Skimmers" are tools used by criminals to capture the data stored inside the magnetic strip of the ATM card. The data can be read using the application embedded on small card readers in proximity to, or on top of, the real card reader input slot. When the device is removed, the data can be downloaded. Although ATM fraud is not the responsibility of the banking sector, it is a major threat that calls for coordinated action on the part of the banking sector, customers and law enforcement agencies. Such fraud undermines customers' confidence in ATMs and discourages greater use of these facilities (Setiawan, 2019).

2.4.2 Cyber-Theft

Cyber-theft refers to the use of computers and communication systems to steal personal data. Hackers use high-powered technologies and computational and programming techniques to gain unauthorised access to the banks' systems and transfer funds to their own accounts. This is a major problem as large amounts of money could be transferred. Credit card fraud is also common, but is frequently under-reported as banks fear losing customers and shareholders. While cyber-theft is the most common and most reported cybercrime, other varieties of computational approaches and techniques for cyber theft include viruses and worms, spamming, phishing and hacking (Kleemans, 2019).

Viruses and worms are common threats to individuals and organisations. Viruses are computer programmes that are designed to damage a computer's systems. Viruses and worms are referred to as viruses because they spread from one computer system to another like a biological virus. A virus attaches itself to a programme and documents stored in the computer system and thus gains access to the system. A worm normally exploits loopholes in the operating system or software.

Spamming is used by criminals to implant a virus in a computer system. It uses electronic messaging systems to disseminate unsolicited bulk messages that promote and advertise products and websites. The most common type of this virus is e-mail spam, which also occurs in other media such as instant messaging, Usenet newsgroups, web search engines, blogs, wikis, online classified ads, mobile phone messaging, internet forums, junk fax transmissions, social networks, television advertising and file-sharing networks (Kaya *et al*., 2020).

Phishing involves sending an unwanted e-mail to a user, falsely claiming to be an established legal enterprise with the aim of scamming them to reveal private information that will be used for identity theft. According to Lee (2018), phishing is high-tech identity theft that not only includes stealing personal information and identity from unsuspecting consumers, but also committing an act of fraud against legitimate and legal businesses and financial institutions (Hassan and Makinde, 2012).

Hacking refers to unauthorised access into a computer or network. An individual who hacks other people's computers is generally referred to as a hacker (Gunkel, 2018). Hackers make use of the loopholes in system software, particularly operating systems, to cause damage to the data and make away with valuable information on a victim's computer. Backdoor programmes are usually installed on victims' computer systems and hackers try to access the resources using password and hacking software. Hackers can also monitor what one does on one's computer and import dangerous files that can damage the functionality of the system. A hacker can install software without the owner's knowledge in order to access information such as passwords and credit card details. Important company data can also be hacked to obtain information on its future plans. There is an increasing tendency to attack cloud resources to gain access to secure information (Abazari *et al*., 2019).

The US Federal Bureau describes cyber terrorism as a politically motivated attack against information security and computer systems and their software. Cyber terrorism causes havoc and the loss of organisations or governments' systems and information. The US Commission on Critical Infrastructure Protection noted that organisations that are vulnerable to cyber terrorism include, but are not limited to, banking institutions, military installations, water systems and traffic control centres (Karabacak *et al*., 2016). Cyber terrorists employ tele-communications devices, the internet and other ICT devices to commit crime.

Cyberstalking involves using the internet to continually harass an internet user. This can be sexual in nature or could be motivated by anger. Harassment is easier when the internet user does not protect their personal information. According to Gibson (2019), cyberstalking employs e-mail, the internet or any ICT device to stalk another person. The term is usually used within the context of online crime, harassment and abuse. The stalker does not usually physically threaten the victim, but follows their internet activities in order to obtain information that they then use to threaten and victimise the person (Chandrashekha *et al*., 2016).

2.5 Causes of Cybercrime and Risk in Nigerian Banks

Information breaches have attained critical proportions in Nigeria, with more dire penalties being meted to culprits as the government essays to curtail the activities of internet fraudsters. Four core factors have been pinpointed as being responsible for cybercrimes in the country, viz: urbanisation; the wealth pursuit; joblessness; and ineffective implementation of cybercrime policies and laws, as well as poorly furnished law enforcement agencies (Okeshola and Adeta, 2013).

2.5.1 Urbanisation

Meke (2012) has recognized urbanisation as one of the main roots of cybercrime in Nigeria. As citizens engage in massive movements from rural to urban settlements in pursuit of more favourable economic prospects and an improved living standard, over-population becomes the natural consequence, and this has led to a very stiff competition for resources, especially amongst the elite. Certain members of these elites ordinarily orientate towards illegal internet activities since they require less capital investment and present the prospect of a quick income. In Nigeria, these criminal elements are commonly tagged “Yahoo Boys”. The Nigerian government therefore needs to confront this problem which is consequent upon rapid urbanisation.

2.5.2 Pursuit of Wealth

The pursuit of affluence in Nigeria is driven by the high levels of disparity between the rich and average citizens, thereby making illegitimate activities a tempting option for them (Okeshola, 2013). Due to the meagre financial investment required by cybercrimes, and because teeming Nigerian youths are unemployed, they easily opt for the fraudulent business as a means of survival. Based on data from the Nigerian National Bureau of Statistics, close to

20 million graduates are unemployed and nearly two million job-seekers enter the labour market each year (Adesugba and Mavrotas, 2016).

2.5.3 Weak Enforcement of Cybercrime Laws

Containing cybercrimes in Nigeria necessitates effective legislation and firm enforcement of laws and regulations which, unfortunately, are absent. This implementation gap is being exploited by the cybercriminals who are thereby encouraged to ply their illicit trade. Nigeria's cybercrime laws are weak and the relevant enforcement agencies are poorly equipped with, or in many instances, entirely lack the necessary digital devices to track down virtual criminals. Remarkably, Emeka (2018) observes that "some of the African countries have been criticized for taking a levity hand in handling cybercrime as their law enforcement agencies are inadequately equipped in terms of personnel, intelligence and infrastructure, and the private sector is also lagging behind in curbing cybercrimes".

2.6 The Effects of Cybercrime on Nigerian Banks

The effects of cybercrime and information breaches in Nigeria include financial loss, loss of reputation and reduced productivity (Martens and Wolf, 2018).

2.6.1 Financial Loss

Cybercrimes impose costs on individuals, organisations and society at large. Anderson *et al*. (2019) identify four categories of financial costs as a result of information security breaches, namely the costs involved in averting cybercrime such as antivirus software, insurance and compliance; those that are a consequence of cybercrime, such as direct losses and indirect costs like reduced competitiveness as a result of intellectual property being compromised; costs in response to cybercrime and breaches, such as compensation to victims (customers and shareholders) and fines paid to regulatory bodies; and indirect costs, including reputational damage to firms, such as the loss of confidence in cyber transactions by individuals and companies, reduced public sector revenue and the growth of the underground economy. Financial fraud in cyberspace is one of the fastest-growing activities in the US, resulting in annual losses of $189 billion (Romanosky, 2016). The cost of application fraud alone is more than $35 billion per year.

The Nigeria Electronic Fraud Forum (NEFF) notes that cybercrime has had negative effects on economic growth, has damaged the country's reputation in the eyes of the world and has had severe cost implication for companies. The Forum adds that this scourge needs to be checked in order to avoid further insolvencies amongst banks and financial institutions. Furthermore, it will undermine Nigeria's efforts to promote financial inclusion. It is estimated that the country's Deposit Money Banks (DMBs) suffered a loss of N203 billion in the past 14 years as a result of electronic fraud. This is likely to be an under-estimate as some cases are not reported. In relation to the declaration of Fadairo *et al*. (2014), 1,461 cybercrime fraud cases occurred, with an Estimated loss of N7.8 billion and an apparent loss of N6.216 billion. The authors further state that in 2013, 855 cases resulted in an Estimated loss of N19.149 billion and a real loss of N485.194 million, while reported cases show that financial institutions are adopting proactive security measures with regard to customers' cards, as well as improved security at corporate level to reduce fraud. The switch from a magnetic stripe for ATM cards to more secured chip and PIN cards in 2009 led to a drastic reduction in e-fraud to the tune of N21.72 billion, with a further decline to N14.96 billion in 2010.

In relation to Smith and Iacobelli (2013), it was said that the Deputy Governor of Financial Systems Stability at the Central Bank of Nigeria, Adebayo Adelabu, stated that 2.4% of banking income was lost to fraud. Consequently, Gates *et al*. (2016) ranked Africa as the continent with the largest number of fraud cases, with sub-Saharan Africa having the highest prevalence (77%) of scams amongst the regions surveyed.

2.6.2 Loss of Reputation

In 2012, the Executive Director of Operations at First City Monument Bank, Mr Nath Ude, observed that cybercrime had damaged the reputation of both the Nigerian government and the banking sector, causing the loss of customer confidence, increased audit costs and a loss of share value. He added that there had been an increase in such crime since 2001 and that Nigeria had come to be associated with cyber fraud (Onifade *et al*., 2019). While fraud and corruption are regarded as the sins of the political class, increased use of the internet via a variety of ICT devices has resulted in an increase in financial fraud, which has caused tremendous reputational damage (Moses-Òkè, 2012).

2.6.3 Reduced Productivity

Cybercrime also negatively affects national productivity. It is estimated that 75% of the loss of productivity in Nigeria in both public and private sectors is as a result of cybercrime. Fraud and theft follow as the most common crimes affecting businesses (Ogunniye and Afolabi, 2014).

2.7 Suggested Possible Solutions for Cybercrime

The Global Trade Review (GTR) notes that the traditional way of dealing with cybercrime and risk management using IT approaches is not effective, and that the financial sector (banks) should build on their IT systems to tailor specific approaches to address each cyber fraud class, considering their peculiarities. The Nigeria Inter-Banks Settlement Systems (NIBSS) Plc and the DMBs observe that fraudsters are becoming more ingenious in circumventing security measures. In a paper titled "e-Fraud: Shining a Light on Insider Abuse", the Chair of the NEFF, Dipo Fatokun advocated for a non-traditional approach, including cyber-attack testing, collaboration, address verification systems, interactive voice response terminals, firewalls, antiviruses, cryptography and ethics, laws and information security policies. These are discussed in the next section.

2.7.1 Cyber-attack Testing

Systems that periodically test banks' readiness to avert cyber-attacks and investigate any occurrences have been adopted by many financial institutions. An example is the Bank of England's CBEST Vulnerability Testing Framework. Nigerian banking institutions are also proposing these types of systems to improve the safety of online banking (Malzahn *et al*., 2020; Ojeka, 2012).

2.7.2 Collaboration

Fighting cyber-crime and electronic fraud requires collaboration amongst banks. Strategies include reviewing the security status of employees whose positions might enable them to commit such crimes and installing technology such as Closed-Circuit Television (CCTV). Moreover, banks should work together to design systems to monitor and access cards as it is known that fraud perpetrated by those within an organisation (insiders) is usually more difficult to detect than that committed by an outsider, and often has higher impact (Bell *et al*., 2019). Since threats could emanate from anywhere around the world, there is a call for international

collaboration, investigative assistance and common substantive and procedural provisions amongst banks.

Addressing a workshop for banks and telecommunications companies organised by the WiniGroup Limited and NIBSS Plc, Mr Shahar Alon, Business Development Manager at Checkmarx, Israel's leading Static Application Security Testing (SAST) developer, said "Nigerian banks and telecom operators must collaborate to protect the economy from cybersecurity threats." He added that collaboration should be an integral part of the job description of any professional in charge of security and that in order to survive, chief information officers (CIOs) "would have to collaborate".

2.7.3 Interactive Voice Response (IVR) Terminals

This device is new technology designed to prevent fraud over voice communication channels by obtaining a "voice stamp" or voice authorisation and verification from the customer before the merchant ships the order. Aside from being a form of IP address checking, the device assists cybercrime detection as it enables organisations to share information and discourages information hoarding, which is common amongst commercial organisations due to fear of competition.

Besides allowing for notification when mobiles are used to transact, the customer is registered on the authentic platform. The transaction request is obtained from the person that initiated the transaction, messages are sent to the authority using the transaction request and a response is received from the authority's device. Once the authority's agent notifies one of the transactions, confirmation is communicated to the initiator. If the agent denies the transaction, the user can communicate the transaction to the initiator (Oberheide *et al*., 2019).

2.7.4 Firewalls, Antiviruses, Anti-spyware Software and Cryptography

Firewalls, antiviruses and anti-spyware software are similar in that they protect a computer system from external invasion and unauthorised access. A firewall is employed to prevent an unauthorised user from gaining access to a computer network and obtaining confidential documents or information. Network firewalls can be hardware devices, software, or both. Antivirus software seeks to detect, thwart and eradicate computer viruses and other malicious software. Anti-spyware also restricts backdoor software such as Trojans from being installed on a computer. Security software should be installed on all computers. Internet service

providers are also expected to deliver a high level of security in order to protect their clients from viruses and malicious programmes (Hsu *et al*., 2012) Cryptography is the science of encrypting and de-crypting information. “Encryption is like sending a postal mail to another party with a lock code on the envelope which is known only to the sender and the recipient”. It is a measure to prevent fraud or the inadvertent corruption of data, loss of data integrity and loss of information (Collins, 2019).

The method of encryption keys comprises host identification and a content identification. They are both integrated with each other to produce the encryption key. In the process, the content identification is known to the block of plain text which is about transmitting via an interface that is unsecure to storage devices. The content identification is attached to ciphertext for transmission to the devices. After transmission, the host devices retrieved the ciphertext where the host identification and the attached content identification are used to re-form the encryption key and thus de-crypt the ciphertext. Also using a time variable to create the encryption key offers a process for restraining the period at which the ciphertext is been decrypted (Weber and Fahrny 2003).

2.7.5 Ethics and Cyber Legislation

Cyber ethics provide moral principles or behaviour in the cyber space, while cyber law refers to the rules and regulations that one needs to comply with when operating in this space. The correct application of cyber ethics and cyber law helps to reduce cybercrime (Umejiaka and Anyaegnu, 2016). It is expected that every computer user follows the cyber ethics and laws guiding their systems. Lazarus and Okolorie (2019) note that governments also adopt particular policies to limit cybercrime. In Nigeria, the Economic and Financial Crimes Commission (EFCC) banned overnight browsing because most fraudulent activities occur at cyber cafés overnight. No quantitative data is available to measure the effectiveness of such policies. Furthermore, the evolution of fixed wireless facilities in Nigeria has provided another platform for cybercrime.

Furthermore, a lack of enabling law makes policing extremely difficult. Nigeria has embraced electronic payment systems to ease transactions for customers and promote e-commerce. The negative impact of cybercrime on the banking sector and businesses in general, and the lack of appropriate policies to guarantee the authenticity of online transactions continues to create

uncertainty in the minds of potential online users and customers (Akinyomi, 2012). ICT tools, such as user identification, a transaction access code (TAC), password electronic tokens and SMS (short message services) alerts are essential pre-emptive procedures to combat cybercrime in the banking sector (Fadare, 2015). However, according to Cavelty (2015), the most important is cybersecurity policy. In curbing cybersecurity issues in Nigerian banks, it calls for compliance with information security standard and policies, and this standard provides the steps and necessary tools for combatting insider threats.

2.8 Information Security Standards Compliance amongst Nigerian Banks

Compliance with information security standards and policies is a vital issue in the banking sector, particularly in the Nigerian context. Information security standards and policies set out measures to protect an organisation's information. Information Security and Standard (ISSsPs) compliance shapes and influences employees' behaviour with regard to organisational information system (IS) resources (Ifinedo, 2012). ISSsPs compliance have not been extensively studied within the Nigerian banking community despite the alarming rate of cyber fraud due to information security breaches (Ibikunle and Eweniyi, 2013). The persistence of cyber fraud and its negative influence on the Nigeria's economy and its banking sector is worrisome. Consequently, Sunday and Bamidele (2014) and Olusola *et al*. (2013) call for an exploration of other non-technological approaches to securing organisational data.

Discussed next is the Nigerian banks' compliance with the global information standard security policies.

2.9 Information Security Standard Governance in the Banking Sector

Fazlida and Said (2015) define ISS governance as controlling and maintaining the information system environment in order to protect, manage and avert any threats to the confidentiality, availability and integrity of an organisation's information. This requires a sound organisational structure and employee buy-in. Similarly, Aceituno *et al*. (2013) define ISSsPs governance as frameworks that assist the board of directors in decision-making in order to fulfil its responsibility to safeguard and protect stakeholders' interests. According to Mattord (2014), ISSsPs governance is a major responsibility of the management and the board of directors in any organisation. It was equally added that it involves structures, processes and relationships which assist the formulation of standards and frameworks to implement and maintain

information security. ISSsPs governance involves putting a set of tools in place to protect and secure the organisation's assets and values.

The majority of the breaches in the banking sector and financial institutions are caused by a failure in information security governance. The Integrity Financial Group (IFG) assists with the effective and sound implementation of information security in the banking sector. Given that there are many information security standards, each with its unique focus in combating information security threats, it starts by identifying where information security governance falls within the organisational hierarchy.

The ISSsPs policies which apply to the banking sector include BS 7799, Payment Card Industry Data Security Standard (PCI-DSS), Federal Financial Institutions Examination Council (FFIEC), ISO/IEC 27002 and the PCI data security standards. These are examined more closely to explain their nature and intent. Standards such as ISO/IEC 27001 mainly emphasise the information security management system, while PCI-DSS was created to manage information security relating to online business transactions and ATM smart cards. Furthermore, COBIT's objective is to secure information and its relationship with project management and information technology governance (Sheikhpour and Modiri, 2012). Many researchers have investigated online banking security and the security issues confronting banking. Studies have also been conducted on frameworks for the governance of information security in the banking sector, information security threats in the banks and the security systems of different types of banks in several countries. However, to the best of the researcher's knowledge, no studies have focused on the type of international standards and codes that Nigerian banks subscribed to. However, studies have identified standards that are useful in securing banks' information: these include PCI-DSS, FISMA, HIPAA, SOX, GBA,BS 17799, ISO/IEC 27002, COBIT and BS 17799/ISO 17799. These standards have been referenced in some of the organisation, particularly in the financial sector.

2.9.1 ISO/IEC 17799 and ISO/ IEC 27001 Series

The International Standards Organisation (ISO) was established in 1947, with its head office in Geneva. Financial organisations are advised to adopt ISO/IEC 17799 as a model for ISSs policies as it assists in assigning roles and responsibilities, and prepares banks for any eventuality (Bahuguna and Pande, 2018). Primarily implemented in Europe and Asia, ISO/IEC

17799 has been adopted as a national standard in many countries, including Australia, the Czech Republic, Finland, Iceland, Ireland, Japan, the Netherlands, New Zealand, Norway, Spain and Sweden. Continually striving towards maturity, ISO/IEC 17799 is already one of the most widely referenced information security frameworks that provides useful information on how to combat cybercrime. According to the ISO, the ISO/IEC 17799 "establishes guidelines and general principles for initiating, implementing, maintaining and improving information security management in an organisation." It does not provide details on how information security should be implemented and maintained (Jusuf *et al*., 2019).

Each organisation is unique and thus confronts different threats and vulnerabilities. Once an in-depth risk assessment has been conducted, an organisation should select the appropriate security controls and measures to manage risk as set out in ISO/IEC 17799. Furthermore, the controls set out in the standard are not organised or prioritised according to any specific criteria. Each control should be given equal importance and considered at the systems and projects requirements specification and design stage. Failure to do so will reduce cost-effectiveness and could result in inadequate security. Finally, the ISO/IEC 17799 cautions that no set of controls will achieve complete security. It thus encourages management to monitor, evaluate and improve the effectiveness of security controls to support the organisation's business objectives (Goosen and Soga, 2019).

It is important to note that the ISO has published international standards that cover a wide range of fields, one of which is information security management. In reference to ISO/IEC 27001 that preceded ISO/ IEC 17799, the standard was primarily established to serve as a standard code for information security practices. Eleven of the guidelines are listed as mechanism controls (Wang *et al*., 2019). Nevertheless, Amarachi and Ajaegbu (2013) describe ISO/IEC 27001 as a standard employed to scrutinise information security frameworks and ensure that the solutions proposed are appropriate.

2.9.2 PCI-DSS

Data security standards (PCI-DSS) are one of the ISSsPs dedicated to enhancing card payment security. PCI-DSS was developed by an information security council, which included American Express. The standard is concerned with bank financial services like Visa International Inc. and MasterCard and ensuring the consistency of data security measures on a

global level. PCI-DSS embraces ISSsPs which cover policies, network architecture, software design and overall information security management standards. It claims to be the globally accepted information security standard which defines the card payment industry standard. This standard was adopted to assist banks to process card payments and to prevent card fraud by increasing their control of the data to prevent too much exposure. It applies to all industries that process and exchange credit (Rasheed, 2014).

Tests for compliance with the PCI-DSS standard can be conducted either internally or externally, depending on the number of annual card transactions. All organisations handling a large number of transactions are required to be annually assessed by independent qualified security assessors. Companies handling a smaller number of card transactions are assessed through a self-assessment questionnaire (Susanto and Almunawar, 2018).

2.9.3 FISMA

The Federal Information Security Management Act (FISMA) was adopted in the US on December 17, 2002 and was known as Title III of the Electronic-Government Act of 2002. The FISMA Implementation Project was established in June 2003 to produce various keys security standards and guidelines required by congressional legislation. These include but are not limited to FIPS 199, FIPS 200, NIST; Special Publications 800-53, 800-59 and 800-60; as well as NIST SPs 800-37, 800-53 and 800-53A. The first phase of FISMA implementation focused on the development of security standards and guidelines, while the second involved the development of accreditation processes for public and private sector entities to provide security assessment services to federal agencies.

The FISMA Project makes comprehensive information on security and assurance guidelines available to organisations and agencies, with the detailed work undertaken by the National Institute of Standards and Technology (NIST). The framework aims to ensure that effective information security controls are in place in relation to resources that support federal operations and that asset protection standard, guidelines and associated methods are developed for information systems. It also implements standards and guidelines, including the requirements expected of information systems operated by an agency or an organisation working on behalf of an agency, apart from national security systems (Bianchi *et al*., 2012).

Managers and all executives of organisations are expected to comply with information security standards. The NIST Federal Information Risk Management Framework (RMF) and the security guidelines set minimum security requirements for non-national security federal information systems authorised by the FISMA. However, Rose (2019) maintains that while it is systematic and repeatable, the subjective compliance evaluation approach defined in the RMF lacks the clarity of a standard quantitative metric in describing the level of compliance required with the FISMA standard.

The FISMA Implementation project develops standards (Federal Information Processing Standards) and guidelines (Special Publications in the 800-series) for non-national security federal information systems, including:

i. Standards to be employed by federal agencies for group information and information systems, to present accurate levels of information security according to a range of risk levels;
ii. Guidelines that recommend the types of information and information systems to be included in each category; and
iii. Minimum information security requirements (management, operational and technical security controls) for information and information systems in each group.

2.9.4 HIPAA

In the Health Insurance Portability and Accountability Act of 1996 (HIPAA, Public Law 104-191), the Security Rule focuses on the protection of Electronics Protected Health Information (EPHI). All entities covered by HIPAA, which includes federal agencies, must comply with the Security Rule, which aims to protect the confidentiality, integrity and availability of EPHI. However, the EPHI is an entity that creates, receives, sustains or transmits in an electronic form, hence it must be protected against reasonably expected threats, hazards and impermissible uses and/or disclosure.

Special Publication 800-66 Revision 1:

i. Educates readers on the information security terms used in the HIPAA Security Rule in order to advance an understanding of the accurate meaning of the standards spelled out in this Rule.

ii. Offers helpful information that may be used in other NIST publications on the topics addressed by the HIPAA Security Rule.

iii. Helps readers to understand the security concepts discussed in the HIPAA Security Rule.

However, this publication does not complement, substitute or supersede the HIPAA Security Rule itself. NIST publications, many of which are required for federal agencies, can serve as voluntary guidelines and best practices for state, local governments and the private sector, as well as assist organisations to select the standards that suit their unique circumstances. NIST security standards and guidelines (Federal Information Processing Standards (FIPS) and Special Publications in the 800 series) which support both HIPAA and FISMA offer a structured, yet flexible framework to select, specify, employ and evaluate security controls in information systems (Moore and Frye, 2019).

2.9.5 SOX

The Sarbanes-Oxley Act (SOX) is federal law for all publicly-held US corporations and it imposes extensive civil and criminal penalties for non-compliance. Its main objective is to establish verifiable security controls to prevent the disclosure of confidential data and to track personnel to detect data tampering that may be fraud related (Badshah *et al*., 2019). The central purpose of the Act is to reduce fraud; build public confidence and trust; and protect companies' and shareholders' data. Its two principle sections are summarised in the next paragraph:

Section 302: Aims to safeguard against faulty financial reporting. It provides tha companies must safeguard their data responsibly in order to ensure that financial reports are not based on faulty data, data that has been tampered with or inaccurate data (Saxton and Neely, 2019).

Section 404: Requires the safeguards set out in Section 302 (as well as other sections) to be externally verified by independent auditors, and that such auditors should disclose possible security breaches that affect company finances to shareholders and the public (Badshah *et al*., 2019).

2.9.6 GLBA

The Gramm Leach Biliey (GLBA) Security Standard aims to provide the data protection security necessary to comply with Rutger's GLBA Security Policy. These standards are mandatory requirements that establish an effective baseline of appropriate system, administrative and physical data controls. Specific information security guidelines and checklists are available to provide guidance on how to comply with these standards. The GLBA standard guideline is presented under the following themes: Network, Host, User's account, Software development and Policy and procedure (Farr and Bailey, 2019).

Network

i. A network-based firewall shall be implemented that denies traffic from "un-trusted" networks and hosts.

ii. Network traffic shall be limited to only those services and ports considered essential, unless exceptions to allow access to required services are requested and granted.

iii. Networks that house devices with GLBA data shall be scanned for vulnerabilities at least semi-annually. Vulnerabilities detected shall be remediated in a timely manner.

iv. Additional security detection tools (Intrusion Detection Systems [IDS]) should be considered in cases where a high degree of GLBA data exists.

Host

i. Devices that process or store GLBA information shall be housed in a physically secure location, accessible to only those with a business purpose.

ii. Security updates and patches shall be applied in a timely manner or automatically, where possible.

iii. Computer system support must monitor for vulnerabilities in their hardware and software.

iv. Where possible, computer anti-viruses shall be implemented and updated in a timely manner or automatically, where appropriate.

v. Where appropriate, a host-based firewall shall be implemented.

vi. Services and applications should be the minimum necessary to accomplish the required business functions: (a) Passwords shall be changed from the vendor defaults and (b) Systems should be "hardened" to a recognised standard, where available.

vii. Individual access to data shall be limited to those needing access for business purposes.

viii. The amount of GLBA information collected and stored shall be the minimum amount required for the efficient and effective conduct of business functions.

ix. Where possible, secure (encrypted) transmission and storage shall be utilised for all devices, including laptops and portable media, where appropriate.

x. Devices processing or storing GLBA data shall log all significant security event information. Logs should be reviewed on a daily basis and be retained for at least 90 days.

xi. Files shall be backed up and tested on a regular schedule and stored in a secure location both on and off site.

xii. Hardware, software and data destruction shall be securely disposed off at the termination of business needs.

2.9.7 BS 17799

This code was first established by the British Standard Institution (BSI) and was initially formulated in 1995 by Britain's Department of Trade and Industry. The first part of the standard, which relates to best practices for information security management systems, was replaced by a new version in 1998 which was later adopted by the ISO and named ISO/IEC 17799. The second part was revised in 1999 and is referred to as BS 17799 version two (BS-2). Titled 'Information Security Management System', it addresses the way ISMS could be implemented, as well as the information security management structure and control. It was adopted as ISO/IEC 2001 and the 2002 version incorporates *plan-do-check* , which aligns with the quality standard ISO 9000 and is also known as the quality assurance model (Susanto *et al*., 2011). According to Disterer (2013), it was noted that organisations certified through BS 17799-2 are rated higher in terms of maturity than those that informally adopt the standard. However, the latter shows higher levels of maturity than organisations that do not implement any ISMS information security frameworks and ensures that the solutions proposed are appropriate.

2.9.8 COBIT

Control Objectives for Information and Related Technologies (COBIT) is an IT tool that enables managers to bridge the gap between control requirements, transaction risk information security issues and technical issues. Gehrmann (2012) compared COBIT and ISO/IEC 17799 in relation to control objectives. The study focused on the mapping techniques employed by COBIT and the possibility of synchronising them. However, Ofusori *et al*. (2018) observes that it might not be cost effective for an organisation to adopt both frameworks. The author thus suggests that when a number of standards are available, a set of ISS that works as an integral part of the model and aligns with it is preferable.

2.10 Benefits of ISSsPs

This section highlights the advantages that accrue to an organisation at various levels when ISSsPs are diligently adhered to through the concerted effort of all stakeholders at the organisational**,** operational, commercial, level and human levels**.** At the *organisational* level, regulatory bodies such as the ISO issue certificates to organisations after they have been evaluated by professionals to ensure their compliance with ISSsPs. These are an important testimony to the organisation's credibility and go a long way in stimulating and maintaining customers' trust. In the case of the *operational* level, the implementation of ISSsPs has great potential to significantly improve a company's operations as they enhance knowledge of such operations from various perspectives. For example, implementing ISSsPs in relation to the organisation's information systems could reveal its weaknesses and how it could be protected. This also assists in risk management for the organisation's survival.

At the *commercial* level, one of the major aims of any profit-oriented organisation is to stand out from the competition, which is a significant factor in achieving growth. Standard and code certification are an important means of distinguishing an organisation from its counterparts as they measure organisational capacity and highlight an organisation's working practices and standards. This in turn enhances clients' and partners' trust and confidence in the organisation.

The implementation of ISSsPs inculcates sound information security practices in employees. It enhances their knowledge and awareness of information security threats and their respective obligations and duties. As time passes, the organization will develop information security consciousness, as well as a security culture and mind-set (Safa and Von Solms, 2016). This study has identified GLBA, SOX, ISO/IEC 17799, HIPAA and FISMA as the adopted

standards. Their selection was due to the fact that they are widely referenced information security frameworks and mostly used in both financial departments and the technical departments of the banking sector.

In summary, international information security standards provide a framework for ensuring business continuity; preserving legal compliance; and achieving a competitive edge. The increasing rate of interest in GLBA, SOX, ISO/IEC 17799, HIPAA and FISMA is due to the fact that there is governing law; a rising awareness of the importance of information security; and to security audits expected by financial sectors and insurance industries.

2.11 Summary of the Chapter

This chapter has substantially reviewed cybercrime and information security breaches in organisations and narrowed it down to specifically the Nigerian banking sector. It also considered information security challenges confronting Nigerian banks, as well as discussed measures to combat cybercrime. Details of information security standards that Nigeria subscribes to and its governance were also considered. The presentation of the theories underpinning this study and how these theories relate to each factor are discussed in the next chapter. The concepts of factors that promote employees' compliance with information security standards and policies are equally considered next.

CHAPTER THREE
CONCEPTUAL FRAMEWORK

3.1 Introduction

This chapter presents the theoretical background to the study. An extensive review in relation to previous studies and information security compliance behaviour theories was undertaken. Seven theories relating to compliance behaviour were identified, namely the theories of *planned behaviour; self-efficacy; protection motivation; social bonding; locus of control; and the social cognitive and agent of paradigm theories*. Three theories viz, the theory of planned behaviour (TPB), self-efficacy theory and protection motivation theory (PMT) were found to fit well with and provide a detailed explanation of the constructs that this study considers. Furthermore, they have all been previously employed by studies on compliance behaviour, particularly employee compliance with organisational policies.

3.2 Underpinning Theory

The TPB, self-efficacy theory and PMT support the conceptual framework proposed by this study and form the basis for its hypotheses. It is proposed that employees' behavioural factors collectively influence behavioural intention and hence behavioural change. In this study, the behavioural change under investigation is employee compliance with ISSsPs.

3.2.1 Theory of Planned Behaviour (TPB)

The TPB has its origins in the theory of reasoned action, which was proposed in 1980 to predict an individual's intention to engage in certain behaviour at a specific time and place. The TPB is employed in this study to explain employees' behaviour in complying with ISSsPs. The key component of this model is *behavioural intent*. Behavioural intentions are influenced by a person's assessment of the likelihood that the behaviour will yield the expected outcome, as well as a subjective evaluation of the risks and benefits of the outcome.

The TPB is one of the leading theories when it comes to motivation in e behavioural studies. It focuses on individual attitudes and behavioural change (Verkoeyen, 2019). The TPB explains the concept of *social influence*, which refers to changes that occur in an individual's feelings, thoughts and behaviour, giving rise to changes in their interactions with other individuals and groups of people. In the same vein, Walsh (2019) declared that a group of people or an individual could be motivated by attitude, which can be broken down into two components:

subjective norms and perceived behavioural control. Nevertheless, attitude could be explained as an individual's positive or negative thinking and feelings about engaging in a certain action. In the same vein, subjective norms explain an individual's perception of what the people who are important to him/her think about certain behaviour.

Perceived behaviour control also focuses on an individual's beliefs regarding the resources required to engage in particular behaviour, as well as its efficacy. The TPB has been extensively used to investigate information system ethics and compliance behaviour, as well as individual compliance with information system security and how it can be influenced. Rosado and Hernandez (2020) investigated two models that have the potential to predict an individual's intention to use an information system, namely the TPB and technology acceptance model (TAM). The authors found that while both models can predict intention to use an information system, the TAM has a slight empirical advantage as it is very easy to apply and could also provide general information about the user. However, the authors did forget to acknowledge that TPB can play both roles in predicting human behaviour in terms of information security standards and policies compliance and the use of information technology.

The TPB has been employed in various fields such as health, information systems and others to successfully predict the behaviour and intentions of users. It states that behavioural achievement depends on both motivation (intention) and ability (behavioural control). Three types of beliefs are identified, namely behavioural, normative and control. Moreover, the theory proposes that human behaviour is guided by three paradigms: behavioural beliefs, normative beliefs and control beliefs. *Behavioural beliefs* consider the outcome of behaviour and evaluate such to determine whether or not to adopt it. *Normative beliefs* refer to expectations and associated motivations in carrying out certain actions, while *control beliefs* describe those factors that facilitate or mitigate the outcome of the action. In sum, behavioural beliefs, normative beliefs and control beliefs give rise to a positive or negative attitude towards an action; perceived and subjective norms; and perceived behavioural control. These lead to behavioural intention to act and consequently the actual action/ behaviour. Further, behavioural intention mediates behavioural factors and actual behaviour and is an immediate antecedent of behaviour.

The TPB has been criticised by scholars for relying on cognitive processes which ignore individuals' feelings prior to engaging in certain actions, as well as the needs that would affect behaviour regardless of expressed attitudes. Moreover, the model does not take into account one's emotions at the intervening or decision-making time. According to Sniehotta (2009), emotions can influence beliefs and other constructs of the model.

3.2.2 Self-Efficacy Theory

Lippke (2020) proposed the self-efficacy theory (see Figure 3.1),) In this theory an individual's perceived ability to competently complete a give task determines his/her motivation to do so. Self-efficacy is considered the primary condition to actualise behavioural change. Consequently, Ifinedo (2012) recognised that the construct of self-efficacy overlap with the PMT and the TPB and thus combined the two theories to examine employees' behavioural intention with regard to ISSsPs. Moreover, Sommestad, Karlzén and Hallberg (2015) included the constructs of perceived norms, perceived vulnerability, perceived severity, response efficacy, response costs and perceived behavioural control in the TPB.

Self-efficacy, which can also be defined as the beliefs of an individual or group of people in their own capabilities, influences the degree to which individuals think or feel about motivating others to bring a specific action to completion Ifinedo (2012). Chen *et al*. (2019) observed that such a belief might make an individual feel optimistic about completing the task. Unlike previous studies, the authors incorporated the self-efficacy and locus of control theories to examine computer safety behaviour. They found that when employees believe that they have the capacity and competency to do so, they are motivated to comply with their organisation's ISSsPs.

Moreover, Ifinedo (2012) included self-efficacy amongst other factors such as attitude towards compliance, vulnerability and perceived severity, which have a positive influence on information security behaviour. The theory of self-efficacy explains how one can transfer self-efficacy in one task to another task under the same conditions.

In the context of information security, self-efficacy can be described as an individual's belief in his/her ability to protect information and information systems from losses, information threats and unauthorised access. The findings of previous studies suggest that people who have

knowledge about information security are much more familiar with the security software used; set security passwords; and frequently practice and conduct information security training. In summary, information security self-efficacy is an indispensable factor that influences information security compliance (Chen *et al*., 2019).

A keen sense of self-efficacy improves human achievement and personal well-being in numerous ways. People who believe in themselves approach tough tasks as challenges to be mastered rather than as threats to be avoided. An efficacious outlook nurtures intrinsic interest and deep engrossment in events. Such people set challenging goals for themselves and maintain strong commitment to them. They heighten and sustain their efforts in the face of failure and quickly regain their sense of efficacy following problems or failure. When they fail, they attribute this to inadequate determination or deficient ability and knowledge, which are obtainable. They tackle threatening circumstances in the hope that they can gain total control over them (Jeno *et al*., 2019).

The most interesting thing about self-efficacy is that it arises from employees' past performance. Employees who successfully execute a task will have more confidence when taking on a subsequent related task than those who failed to complete that or a similar previous task. This might explain managers' use of self-efficacy to assess prospective employees by setting challenging assignments (Afzal *et al*., 2019).

The three basic sources of self-efficacy are vicarious experience; verbal persuasion; past performance and emotional cues. These are integrated into the conceptual model in Figure 3.1.

Verbal persuasion can be simply explained as verbally instilling self-efficacy in others by convincing them of their ability to carry out a task. The best way for a leader or manager of an organisation to adopt verbal persuasion is through the Pygmalion effect, which is explained as the understanding that one has fulfilled his or her dream which he or she believed would come true (Spengler, 2020). The Pygmalion effect has been adopted in the workplace and studies have shown that when a manager or supervisor has confidence in employees' abilities to carry out a task, they tend to perform it at a higher level. However, the supervisor's persuasive power will depend on his/her credibility. The previous relationship between employees and the supervisor also influences the level of success (Farahnak *et al*., 2020).

Bandura posited that *emotional cues* dictate self-efficacy. Employees who expect to fail when given a task may experience flushed faces, sweaty palms, etc., although the symptoms differ from one person to another. If this continues, it may be associated with deficient performance. Self-efficacy is known to have a relationship with emotion. It is important to note that goal-setting theory and self-efficacy have something in common and complement each other. When a manager or supervisor sets tough goals, employees achieve higher self-efficacy.

Self-efficacy belief has a strong influence on the choices that employees make, as well as the courses of action they try to follow. People often only engage in tasks if they think they have the ability to do so and have confidence in their ability. They try to avoid those tasks that they do not feel they have the capacity to execute. Goode (2020) noted that, "*experience* is what an individual chooses to attend to". If this is true, self-efficacy beliefs that influence decisions or choices are equally capable of determining one's experience and offer an opportunity for an individual to exercise control over events that affect his/her life. Personal belief in one's competence can also sometimes determine the degree of effort an individual invests in a task; the extent of his/her perseverance when faced with obstacles; and the degree of resilience when encountering tricky situations.

It is therefore clear that personal and individual self-efficacy beliefs stem from self-perceptions of past achievements and resultant knowledge.

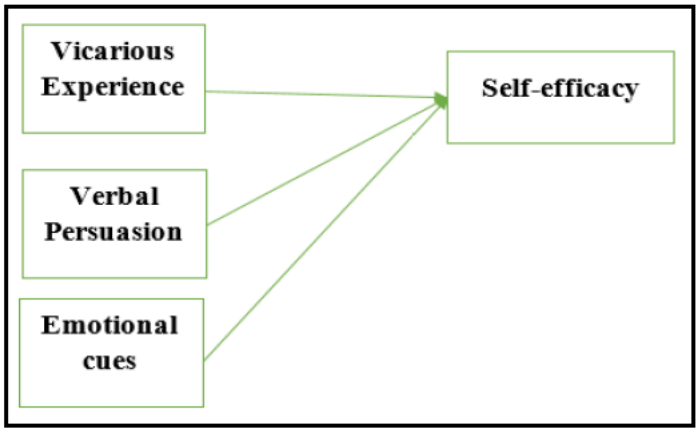


Figure 3.1: Sources of Self-Efficacy (Source: Lippke (2020)

This theory is very important to this study because it explains the nature of normative beliefs, which has a strong influence on the choices that employees make, as well as the courses of

action they try to follow. Therefore, employees will comply with information security standards and policies once they are sure of the effectiveness of compliance and seeing others doing the same. Although the theory did not envelop the entire construct in this study, to some extent it has been able to explain extensively the perceived severity of penalty and normative beliefs.

3.2.3 Protection Motivation Theory (PMT)

Protection motivation theory (PMT) can be defined base on the users protecting themselves on the basis of these three factors: the *perceived severity* of a threatening event, the *perceived probability* of the occurrence, or *vulnerability*, the efficacy of the recommended *preventive behaviour*, and the *perceived self-efficacy*.

PMT is one of the leading theories when it comes to motivation in the field of health beliefs, as it has always been used to predict behavioural changes in the field of information security policies using the human factor. Perceived severity of penalty is considered as one of the components of PMT, which involves the physical and psychological harm a potential threat might cause. In the context of this study, it means potential threats that would have negative consequences on the organisation caused by information security breaches, either from insiders or those outside the organisation. The assumption is that if an information security breach occurs as a result of an employee exposing and leaving passwords in visible places or some other careless behaviour and this becomes a problem for him/her and his organisation, he/she will not exhibit such behaviour in future.
According to Cohen-Louck and Levy (2020), Perceived vulnerability refers to the probability that a negative event will take place if no one takes measures to counter it.

Ifinedo (2012) employed the TPB and PMT to investigate information system security compliance and found that factors such as self-efficacy, attitude towards compliance, subjective norms, response efficacy and perceived vulnerability positively influence employees' behavioural compliance intentions towards ISSsPs. However, the data analysis did not support response costs and perceived severity.

The PMT is one of the leading theories when it comes to motivation in the field of health beliefs. It involves two appraisals: threats and coping with threats. Appraisal involves the

evaluation of fear that occurs due to individual perceptions and how a person feels due to the situations and circumstances surrounding him or her.

Consequently, the appraisal of threats covers two issues:

(1) *Perceived vulnerability*: This refers to the extent to which an individual believes that negative circumstances will occur if measures are not taken to control such circumstances.
(2) *Perceived severity*: This is concerned with the extent to which physical and psychological phenomena measure the susceptibility of employees in an organisation to information security breaches and the potential harm to its information security.

Coping appraisal also covers two issues:

(1) *Self-efficacy*, which in this context demonstrates individual opinion or judgment of the coping response action, and
(2) *Response efficacy*, which is how effective the recommended coping response is in reducing threats to an individual.

Self-efficacy is very powerful when it comes to predicting intentions to comply with certain behaviour and is in line with the context of employees' belief in their ability to cope with certain behaviours, that is, compliance with ISSsPs and organisational procedures (Siponen, Mahmood and Pahnila, 2014).

Some studies on employees' and home users' computer usage suggest that preventive behaviour influences threats and coping appraisals, which are indispensable elements of the PMT. When a group or individual perceives an incoming threat, they form a belief on its severity. This can be evaluated against beliefs about the efficacy of potential responses (Anderson and Agarwal, 2010). However, these factors are not sufficient to measure the factors that drive the information security protection intention of the individual computer user (Nguyen and Kim, 2017).

Siponen *et al*. (2014) proposed a multi-theory model to explain employees' compliance with information security policies. The model combines the PMT, the Theory of Reasoned Action and the Cognitive Evaluation Theory. The results showed that perceived vulnerability to potential security threats, employees' attitudes and social norms all had a significant and

positive effect on employees' intention to comply with information security policies. Intention to comply also had a significant effect on actual compliance.

Thus, this study assumed that these constructs influence employees' behavioural intention, which in turn influences their intention to comply with ISSsPs. The *protection motivation theory* is worth mentioning here as this theory provides an explanation of the intention of the employee to comply with ISSsPs and discusses how normative beliefs, and perceived effectiveness together with the probability of detection and expected penalty, predict information security standards and policies compliance.

3.2.4 Social Cognitive Theory

The social cognitive theory has been widely used to explain human behavioural dynamics and can be adapted to explain the role of social and personal factors. It states that employees can be actively involved in their own development and obtain the desired results when they believe that the behaviour or action is under their control (Schunk, 2020). However, Hooper and Blunt (2020) separated the social cognitive theory into two components: locus of control and self-efficacy. Yoon *et al*. (2019) employed the social cognitive theory to investigate the relationship among self-efficacy in information security, information security behaviour and motivation to strengthen security efforts. They also explored antecedents to individuals' self-efficacy belief in the domain of information security. The results suggest that the consequences associated with violating the information security policy influence the extent of compliance. They also suggest that home computer users' intention can be determined by combining social cognitive and psychological elements (Nguyen and Kim, 2017).

This theory emphasised the role of social and personal factors in this context of normative belief which stated that employees will follow the same compliance when seeing the other doing it. The context of normative beliefs was not well articulated and the intention to comply with actual compliance was not well addressed. Therefore the theory cannot be incorporated into the study.

3.2.5 Social Bonding Theory

The Social Bonding Theory (SBT) refers to the existing bond, otherwise called a social bond, amongst a group of people or between two individuals. Sims (2012) states that when a group

of people or an individual builds on such bonds, this leads to antisocial and anti-establishment habits or behaviours and a means of identifying with an organisation's values, while commitment means an individual or collective effort to support the organisation's ISSsPs, as well as the energy committed to moving the organisation to greater heights. This could also refer to building a relationship with employees. Ifinedo (2013) alludes to Personal norms as the values of a group of people or individuals in a company and their respective views on compliance with ISSsPs.

Ifinedo (2014) investigated employee behavioural intention to comply with ISSsPs using the SBT. The findings revealed that the social bonds which employees form at the workplace influence their intention to comply with information security policies. Similarly, employees' loci of control, capabilities and competences related to IS security issues affect ISSsPs compliance behavioural intentions. The overall variables in the model showed that social, organisational and psychological factors could motivate employees to comply with ISSsPs in the workplace. Yazdanmehr (2020) stated that social influence contributes to shaping information system security compliance behaviour.

Jiang *et al*. (2020) adopted the SBT to explain adolescent behaviour with regard to cigarette smoking, using a longitudinal design. The study found that adolescents' ties to aspects of conventional society are very important in constraining deviant behaviour and more importantly, commitment and belief. Although this theory address intention to comply with information security, it would have been good if the model had looked at individual compliance, not the group of people in the workplace. The factors in this study are individual perceptions towards complying with information security and standards of the banking sector. Social bounding emphasises the bond between one or more employees in the workplace, as Sims (2012) supported that such bond, if it exists in an organisation, will move the organisation forward. The theory ascertains some level of compliance when normative beliefs are brought in. Contrarily, if this bond exists in terms of compliance with information security standards and policies, the place of severity of penalty will be denied and such a bond might not allow the manager to place a sanction on the offender who violates the information security of the organisation. Therefore, this theory will not be useful in this study.

3.3 Justification for the Selected Theories

While all the theories reviewed would have been useful for this study in one way or another, three were selected, namely TPB, the theory of self-efficacy and PMT. This is due to the fact that these theories have been extensively used in research on compliance with ISSsPs. Furthermore, they explain how an individual behaves when he/she is expected to carry out a certain action or behaviour (applicable in the context of information security). The PMT measures the coping behaviour of an individual when he/she is aware of an information security threat. This behaviour directly influences his/her response and level of willingness to comply with the recommended behaviour (ISSsPs) (Van *et al*., 2019). The theory of self-efficacy explains the extent to which the individual believes it is possible to implement the protective behaviour and the effectiveness of such behaviours. The TPB strengthened the study by explaining human behaviour. It is primarily designed to examine an individual's attitudes, which are based on belief, intention and action. The central focus of the TPB is intention to carry out a specific behaviour (Hall *et al*., 2019). Furthermore, the TPB theoretical framework includes the role played by attitude in adopting behaviour (Oteng-Peprah *et al*., 2020).

The three theories thus conclude that an individual's behaviour is within his/her control as attitudes or beliefs are based on a set goal and the outcome of the action. This study integrates the theory of self-efficacy. However, TPB and the PMT are explained in the framework. These three theories are useful as they all explain the behaviour and attitude of an individual or employees when change occurs or they are expected to implement security measures (compliance with ISSsPs).

The models developed by other scholars that have used the three theories are presented in Figures 3.2 to 3.5.

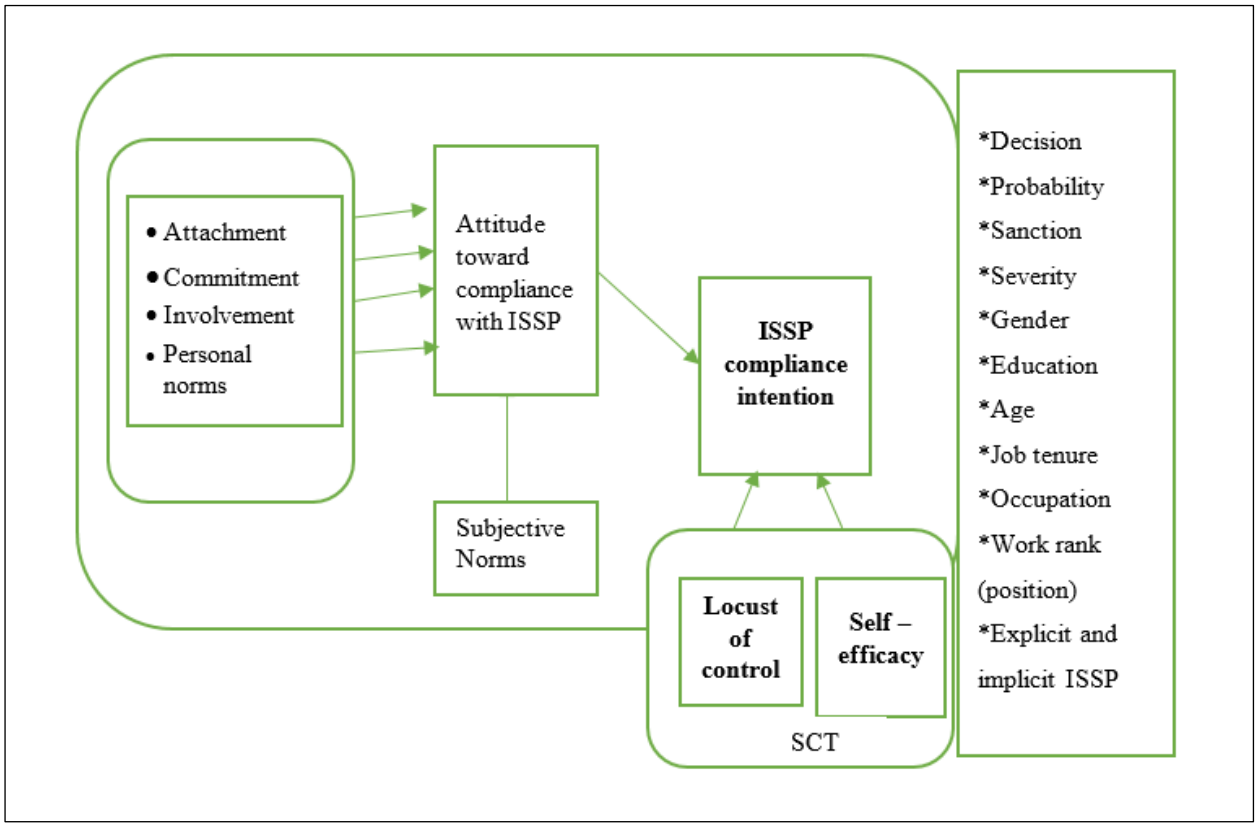


Figure 3.2: Ifinedo's (2014) Model

Vance *et al*. (2012) investigated the factors that motivate compliance with information security policies, using vulnerability, perceived severity, reward response efficacy, self-efficacy and response cost. The authors employed PMT to explain the effect of these factors and their impact on employee compliance. Ifinedo's (2014) study on ISSsPs compliance behaviour intention was based on the theories of social influence and social bonding and the social cognitive theory. The author used the TPB to show that previous theories have focused on Deterrence theory.

Liu *et al*. (2020) used the PMT to determine employees' behaviour towards compliance with information security policy. The authors employed sanction threat appraisal, coping appraisal, normative beliefs, habit and reward as mediators to establish employee attitudes in this regard. The conceptual model developed by Xiao *et al*. (2020) is presented in Figure 3.3, which is made up of the behavioural factors that promote intention to comply with information security policies.

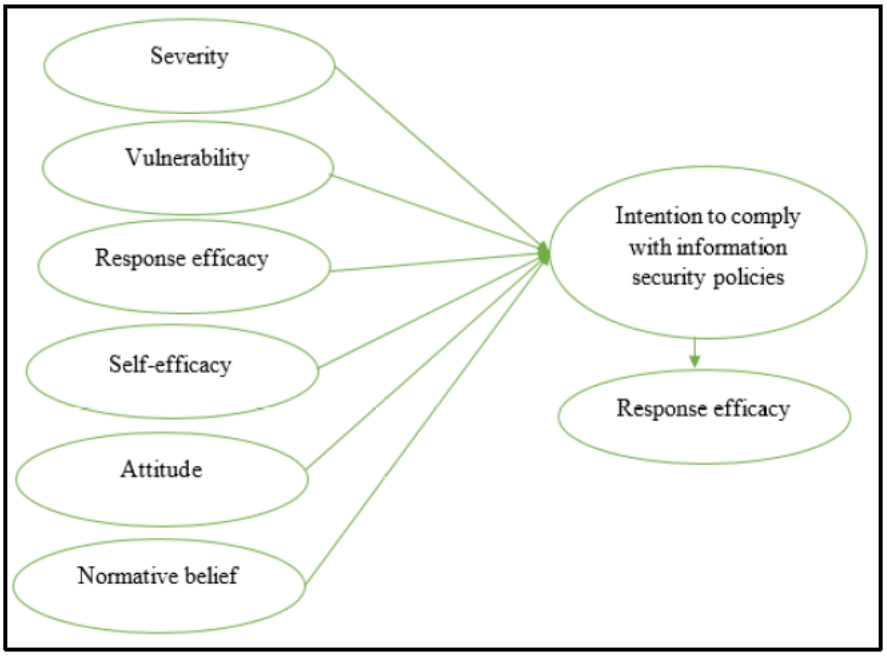


Figure 3.3: Xiao et al.'s (2020) Model

Safa *et al*. (2016) investigated user information security consciousness in an organisation. Using SEM as a statistical tool, they found that information security awareness; information security organisational policy; information security experience and involvement; attitude towards information security; subjective norms; threat appraisal; and information security self-efficacy have a positive effect on users' behaviour. However, perceived behavioural control was not found to significantly affect their behaviour, while PMT and TPB were employed for the research model. Figure 3.4 shows the conceptual model developed by Safa *et al*. (2016).

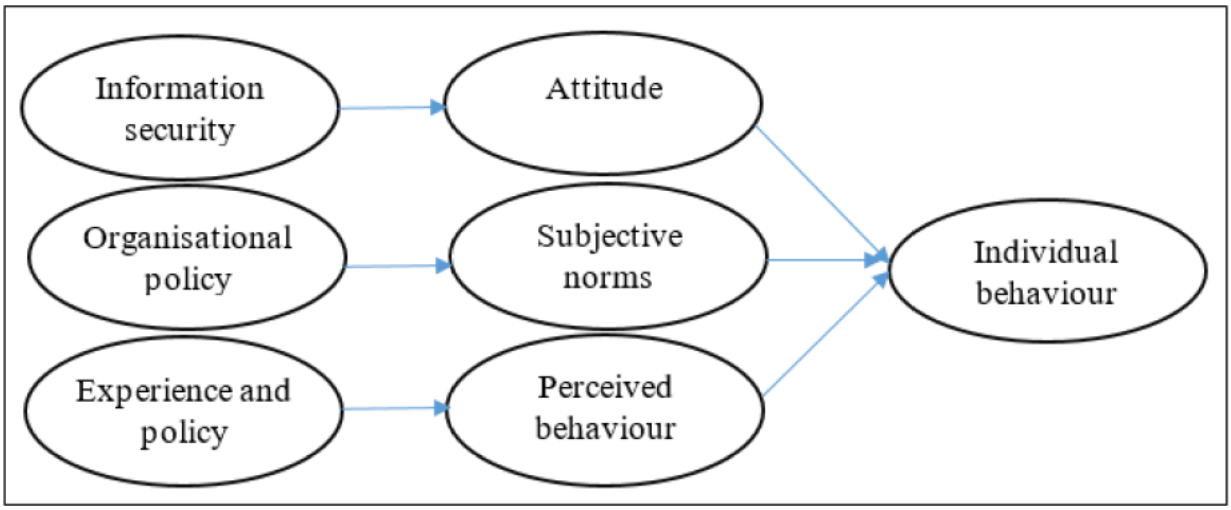


Figure 3.4: Safa et al.'s (2016) Model

Siponen, Pahnila and Mahmood (2010) employed normative beliefs; threat appraisal; self-efficacy response efficacy; visibility deterrence; and rewards as constructs, with PMT as the theoretical framework to investigate why some employees comply with information security policies and others in the same organisation do not. The overall results suggested that employees in each of the organisations investigated need to be motivated by both managers and their peers in order to comply with information security policies. Only one theory was employed but combining a number of theories would enable better understanding. For example, Yazdanmehr and Wang (2016) adopted the norm activation theory, the social norms theory and the ethical climate literature to propose a model that shows how related personal norms could be developed and how this could change employees' behaviour in terms of information security compliance. Given that compliance with information security is necessary behaviour, employees need to develop the requisite attitude (Guhr *et al*., 2019). Figure 3.5 contains the influence between the two factors.

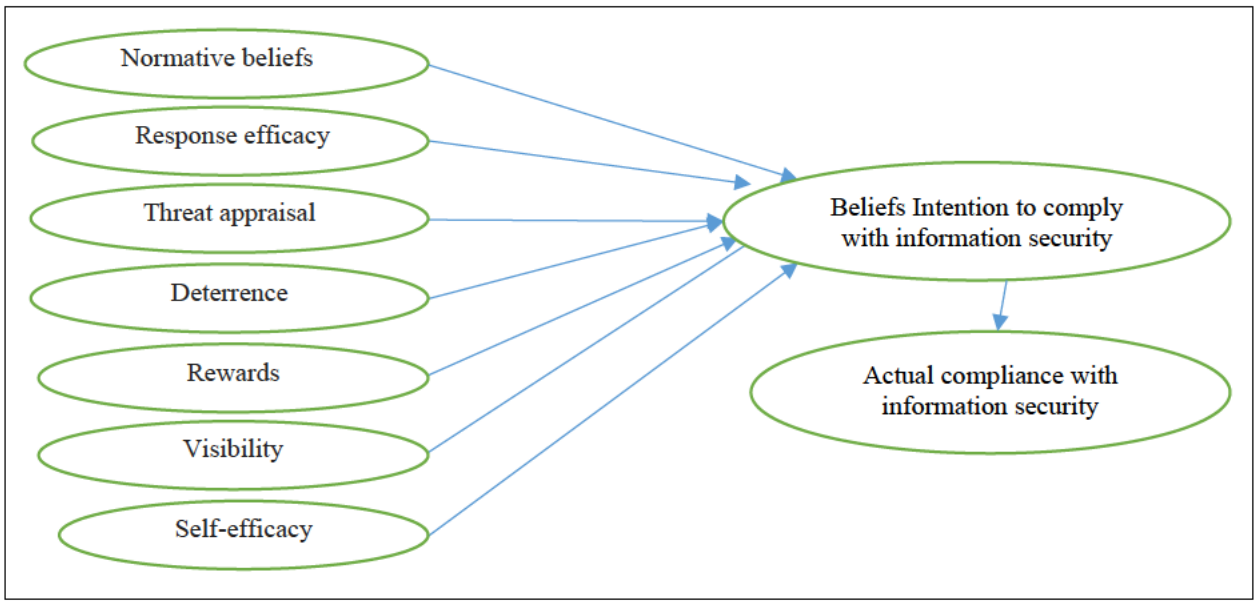


Figure 3.5: Siponen et al.'s (2010) Model

Vance *et al*. (2012) found that past behaviour influenced employees' decision to comply with information security policies. They integrated habit with the PMT to explain information security compliance. The results suggested that habitual IS security compliance strongly reinforces the cognitive processes theorised by the PMT, as well as employee intention for future compliance. The authors also found that all the components of the PMT influenced employee intention to comply with information security policies.

3.4 The Conceptual Framework of the Study

Self-efficacy, which can also be defined as the beliefs of an individual or group of people in their own capabilities, influences the degree to which individuals think or feel about motivating others to bring a specific action to completion. According to Chen *et al*. (2019), the degree of self-efficacy will dictate how high a goal such employees set for their performance. Some studies have shown that setting a difficult goal instils confidence in employees (Locke and Latham, 2019). Self-efficacy will allow employees to believe that their compliance with information security is possible if the employees truly wish to carry it out. This theory will take care of normative belief perception biases. Ifinedo (2012) recognised that the construct of self-efficacy overlaps with the PMT and the TPB and thus combined the two theories to examine employees' behavioural intention with regard to ISSsPs. The two theories will be useful as these take care of the perceived effectiveness of ISSsPs certainty of detection, perceived severity of penalty and awareness of information security threats.

This study employed constructs from other studies that have been validated and used to examine how the employees in a particular organisation comply with the information security of their organisation. However, the use of these constructs (penalty, detection, beliefs, awareness) has not been prominent in the context of Nigeria's banking sector. In the Nigerian context, these mentioned constructs have not been used to predict the employee's behaviour in terms of information security standards and policies compliance. The listed constructs are now modified to include other constructs such as the effectiveness of ISSsPs and perception biases. Figure 3.6 shows the modified framework of this study.

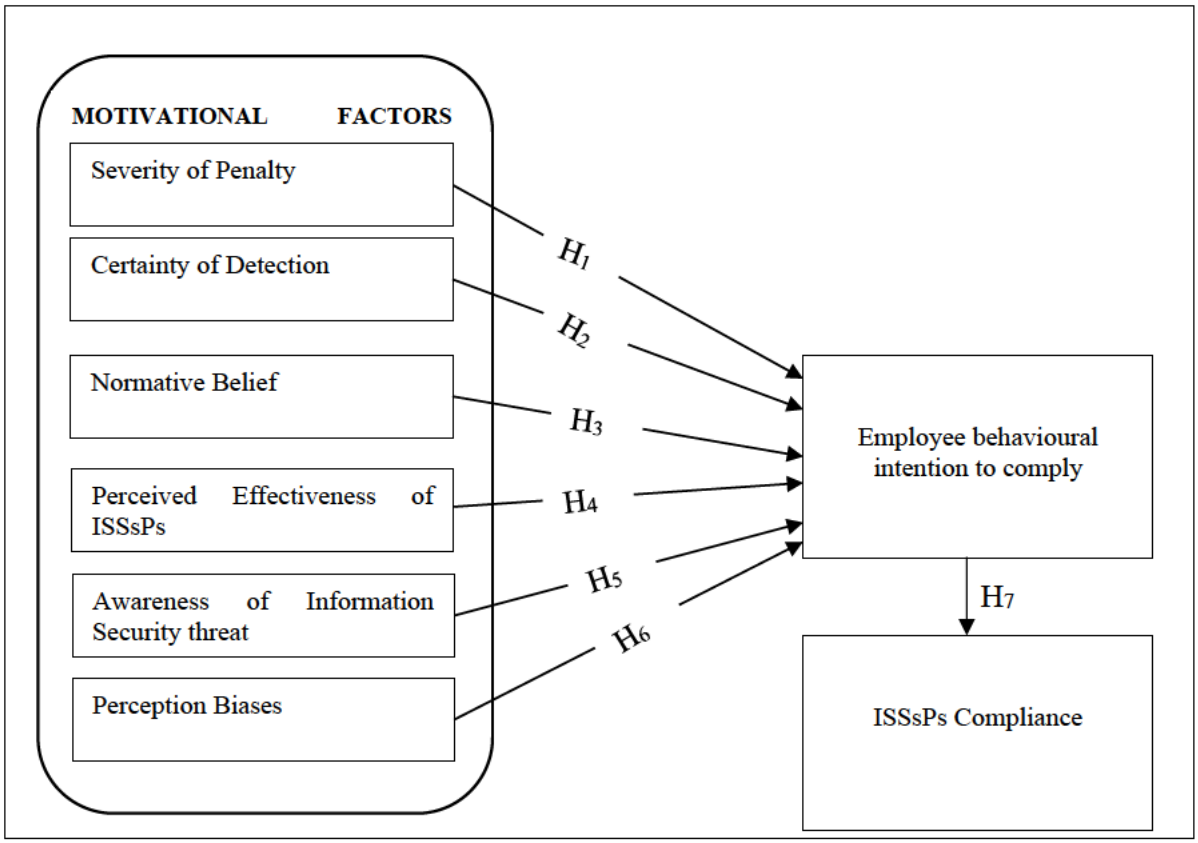


Figure 3.6: Conceptual Framework (Source: Author's own)

3.5 The Conceptual Framework and the Construct

The dependent variable in this study's Conceptual framework as seen in Figure 3.6 is ISSsPs compliance. It is the final consequence of the contingent factors that influence the mediating variable before actualisation. It is the actual execution of the action in the human behavioural chain. In this study, it is operationalised as employees' actual compliance with the stated ISSsPs. Actual information security compliance is expected to be influenced by motivational factors (severity of penalty, certainty of detection, normative beliefs, perceived effectiveness and awareness of information security threats) and mediated by the employee's behavioural intention to comply with ISSsPs.

Muller (2020) posits that an individual's actual behaviour is a reflection of his/her intention to perform a certain behaviour. These intentions relate to the individual's motivation. In order to accurately predict behaviour, antecedent factors have to be examined in relation to its context. Furthermore, the antecedent factors must be stable and must be accurate with perceived

behavioural control. When subjects have control over their decision to perform certain behaviour, intention is sufficient in predicting behaviour (Olya and Han, 2020).

Ameen *et al*. (2020) found that an employee's behavioural intention has a strong relationship with actual behavioural compliance. Liu *et al*. (2020) predicted actual compliance behaviour using self-efficacy and information security compliance and found that self-efficacy and the information security climate only explained about 26.5% of the variance in actual information security compliance. They therefore suggested that other variables be added to the model for better prediction of actual information security compliance. Based on this recommendation, the current study includes motivational factors as the antecedents of employee behavioural intention which have the tendency to predict actual compliance with ISSsPs.

The study classified the factors that influence employees' decision to comply with ISSsPs into intrinsic and extrinsic factors (Herath *et al*., 2014), depending on their nature. *Intrinsic* factors are internally induced, while e*xtrinsic* factors are externally induced. The intrinsic factors which are hypothesised to be antecedents to employees' behavioural intention are perceived effectiveness of ISSPs; awareness of information security threats; and perception biases. Conversely, the extrinsic factors are severity of penalty, certainty of detection and normative beliefs.

As explained earlier, these factors can be understood from the theoretical explanations of TPB, self-efficacy theory and PMT. Severity of the penalty, certainty of detection and perception bias are behavioural beliefs that consider the outcomes of an action in evaluating the essence of carrying it out. Normative beliefs, as conceptualised by this study, also stem from the TPB's explanation. These factors lead to the behavioural intention to act, conceptualised as intention to comply in this study and finally, to actual action. The actual action/behaviour is conceptualised in this study as an organisation's compliance with ISSsPs.

The following section examines the factors (constructs) that motivate employees to comply with ISSsPs. These factors were used to form the constructs of this study that influence the actual compliance.

3.6 Empirical Review of Motivational Factors that Influence Employees' Compliance with ISSsPs

This section discusses previous studies on the relationship between the motivational factors that influence employees' behavioural intention and ISSsPs compliance. As noted previously, end-user behaviour, which has not been the subject of many studies, impacts ISSsPs compliance (Ifinedo, 2014). Indeed, it has been estimated that individual bias in risk estimation and inflated security optimism account for about 35% of security breaches (Ponemon Institute, 2013) An extensive review of related studies revealed that the factors discussed in the next section are the most pertinent (Alotaibi, 2019).

Employees' behaviour plays a significant role in securing and protecting information and the confidentiality of organisational information. Li *et al*. (2019) identified peer behaviour cues that can shape the behaviour of employees in complying with ISSsPs. In addition, Klein and Luciano (2016) investigated information security behaviour amongst Brazilian users and identified threats sustainability, threats severity, certainty of detection, punishment severity, safeguard effort and satisfaction as behavioural factors that can promote positive information security behaviour.

In line with the aforementioned studies, in this study, behavioural factors are referred to as motivational factors and these include severity of penalty, certainty of detection, normative belief, perceived effectiveness of ISSsPs, awareness of information security threats and perception biases.

3.6.1 Severity of Penalty, Employee Behavioural Intention and ISSsPs Compliance

The severity of the penalty imposed on employees when there is a security breach can influence their intention to comply with security standards. Best (2014) termed this an organisational sanction, involving disciplinary action to increase ISSP compliance. Moreover, Brown (2017) found that penalties, whether formal or informal, do not have a significant effect on employee compliance with information security. Brown (2017) suggests that this might be due to the fact that fear of punishment might not be sufficient to cause an employee to comply with an organisation's ISSsPs.

Consequently, crime and its deterrence have been extensively addressed in the literature. Recently, research on optimal punishment has been integrated into the agency theory, on which Coffee (2020) developed a model for penalties in the corporate crime context. In the same vein, Wiafe (2020) examined the role of penalties in the context of collective action, as penalties play an indispensable role in the context of pro-social acts. These studies reveal that sanctions assist in preventing anti-social behaviour.

Deterrence measures are the main tools employed to reduce information threats and computer abuse (Willison and Warkentin, 2013), whereas as the degree of punishment increases, an individual is expected to be less motivated to engage in deviant behaviour. Park (2013) found that the severity of the punishment is significantly related to attitudes to software piracy. According to Vance (2020), if an individual has an opportunity to violate an organisation's policies, his or her actions depend on a rational calculation of the costs and benefits. Numerous studies have explored the similarity between information security policy violation in an organisational setting and criminal action. This fundamental area of information security research explores deterrence theory, rational choice and social control (Lanfear, 2020).

According to Pham, Brennan and Richardson (2017), employees consider the certainty and severity of punishment in deciding whether or not to violate the rules. In a security compliance context, organisations might employ security mandates and disciplinary action to manage and motivate compliance (Coglianese, 2020). Hence, communicating the severity of penalties for rule-breaking behaviour to employees has been regarded as an effective strategy to improve compliance with ISSsPs.

Based on the discussion, the researcher is of the view that the severity of punishment, when communicated to the employees, will significantly influence employee behavioural intention to comply with ISSsPs. The variables can been seen together with others in Figure 36.

3.6.2 Certainty of Detection, Employee Behavioural Intention and ISSsPs Compliance

An employee's heuristic potential to estimate the likelihood and importance of cyber fraud detection can influence his/her compliance rate (Pfleeger and Caputo, 2012). However, the common risks associated with cyber theft are poorly documented and often under-estimated compared to those related to hacking, which are over-estimated. While deterrence theory-based

security measures are mainly based on fear of punishment, the effectiveness of threats of punishment to achieve security compliance remains open to debate. Cheng, Li, Wenli, Holm and Zhai (2013) concluded that fear of penalties has a significant impact on security behaviour and that if employees perceive a high certainty of being caught for violating security policies, they are more likely to comply (Hu *et al*., 2011). The researcher is of the opinion that certainty of detection will significantly influence employees' behavioural intention to comply with ISSsPs and policies.

3.6.3 Normative Beliefs, Employee Behavioural Intention and ISSsPs Compliance

The concept of subjective norms states that an individual's behaviour is based on the views of people who are important to him/her, as well as perceived societal demands to act or not act upon behaviour (Wang, 2020). They have also been defined as having control over perceived pressure and the intention of doing or not doing the act. According to Bech-Larsen, Chan and Tsang (2012), subjective norms refer to other people's perceptions of the person's ability to act or not. Wiafe (2020) notes that following much debate on the role of norms in predicting behaviour, there is consensus in the literature that social norms impact actions in immediate and important ways. This resulted in numerous projects over the past decade that investigated the role of such norms in regulating social practices.

Dealing with information security threats and ensuring that each user understands their role in mitigating such threats is an integral part of information security management. Organisations are made up of employees, their interactions within organisational processes and the system. Each employee has an assigned role and responsibility to ensure information security. Nevertheless, securing internal information is a major goal of everyone in the organisation, hence every employee is expected to adhere to relevant security practices. Furthermore, employees at all levels of the organisation are expected to prioritise information security as the information of the company is the company itself (Soomro, Shah and Ahmed 2016). In addition, information security managers have specific responsibilities because of their expert knowledge.

Previous studies have also used social norms as a measure of normative beliefs (Ghouri, Khan and Kareem, 2016). Normative beliefs reflect normative expectations of peers or colleagues (Bamberg, 2020). On the other hand, peer behaviour addresses how employees' compliance

rate is influenced by the approval and/or disapproval of their peers. The cross-fertilisation of security training and awareness amongst co-workers and subjective norms, i.e., considering what is appropriate, also constitutes peer behaviour. Finally, the social environment or the influence of important people may impact behaviour (Peterson, 2014; Merhi and Midha, 2012). There is an abiding normative belief amongst employees that cyber threats will be less likely when there is significant control of the causative environment (Nasir *et al*., 2020). The author equally suggests that individuals adopt behaviour based on their interaction with one another, while employees who are overly optimistic may over-estimate their control and not readily comply with ISSsPs. With respect to compliance with IS security policies and guidelines, colleagues' or managers' positive attitudes to complying with the rules may guide other people's attitudes, leading to positive behaviour (Hu, Dinev, Hart and Cooke, 2012).

Several studies have found that normative beliefs have a tendency to influence the behavioural intention of individual employees. Following this, Karjalainen (2020) investigated the behaviour of employees in relation to IS security compliance companies and found that normative beliefs had a significant effect on intention to comply with IS security policies. Ghouri *et al*. (2016) also found that normative beliefs had a significant effect on improving employee behaviour amongst small- and medium-sized firms. This study thus hypothesised that normative beliefs will significantly influence employees' tendency to comply with ISSPs. It also posited that employees' behavioural intentions will mediate the relationship between normative beliefs and ISSsPs compliance.

3.6.4 Perceived Effectiveness of ISSsPs Compliance, Employee Behavioural Intention and ISSsPs Compliance

Employees' perceptions of the effectiveness of ISSsPs compliance can influence their readiness to comply with security standards. This is described as self-sanction by Tyler and Balder (2005), who observed that there is an intrinsic desire to comply with ISSsPs. When employees perceive the effectiveness of their compliance with information security measures, this may motivate them to continue to comply. However, Williams (2019) hypothesised that the effectiveness of an action has an effect on one's attitude towards it. When the first action is effective, people are generally motivated to perform further positive actions. These constructs are very important in predicting employees' compliance with ISSsPs.

3.6.5 Perception Biases, Employee Behavioural Intention and ISSsPs Compliance

Perception bias, in particular optimism bias, is one of the constructs employed by this study to predict employees' compliance behaviour. According to Hewitt and White (2020), optimism bias is defined differently depending on the individual's perceptions or expectations and the real outcome of the event. For example, if a person's perception or expectation of the outcome is better than the reality, the bias is said to be optimistic. However, if the outcome is better than the perception, the bias is considered to be pessimistic. The degree of optimism bias can be measured empirically by comparing the person's perception before an event takes place with the outcomes that transpire. Holt (2020) describes this phenomenon as users' refusal to believe that their organisations can be targeted by malware. This bias can mitigate against their compliance.

3.6.6 Awareness of Information Security threats, Employee Behavioural Intention and ISSsPs Compliance

Information security awareness refers to an employee's general knowledge about information security, as well as knowledge of his/her organisation's ISSsPs (Bulgurcu, Cavusoglu, and Benbasat, 2010). A lack of understanding can affect employees' perceptions of risk and their subsequent decisions. In line with ISO 27002, every organisation's information security policy should be periodically updated. However, this security measure will fail if it is not communicated to employees. Organisations using ICT tools need to implement the correct tools to ensure availability, confidentiality and integrity of information. Da Veiga and Martins (2015) state that information security awareness is one of the four tools used to guard against security threats.

Kim *et al*. (2019) defined awareness as the vital information that needs to be communicated to employees. Information security policies should include the definition of information security; management statements; intentions supporting the goal and principles of information security; explanations of specific security policies, standards and compliance requirements; definitions of general and specific responsibilities for all aspects of information security; and an explanation of the process to report suspected security incidents. In the same vein, corporate IS security policies need to be drafted with IS security objectives, strategies and other policies in mind (Safa *et al*., 2015). All these are expected to be effectively communicated to employees.

The recommendations of Burns (2019) with regard to security awareness include security being part of job descriptions; recruitment screenings; confidentiality agreements; information security education and training; reporting of security incidents; security weaknesses; software malfunctions; and disciplinary processes. It is equally important to note that employees need to feel that security procedures are effective and that they can point to any weaknesses. Finally, employee awareness of security threats is vital, and both employees and users are expected to have full knowledge of such threats. Each user of the information system should be familiar with the organisation's security policies and procedures, and should be able to employ these in their day-to-day activities. From an organisational perspective, it is expected that every organisation conducts comprehensive information security training and awareness campaigns, and that there are regular information security briefings. Furthermore, newsletters/circulars should be produced to update employees on any changes to organisational ISSsPs, while the organisation should regularly review and update its awareness programme.

Information security awareness is amongst the strategies that managers should adopt to change the security environment of an organisation (Humaidi and Balakrishnan, 2015; Bauer and Bernroider, 2017). A study on the relationship between general security policy awareness and security policy found that creating security awareness amongst employees has a positive, significant effect on employees' compliance with an information security policy Williams (2019). The study further revealed that employees' outcome beliefs influenced their overall assessment of consequences, which in turn positively impacted their tendency to comply with ISSsPs, suggesting that information security awareness programmes should be designed to reinforce employees' outcome beliefs and create a security-aware culture. Many organisations believe that internal security threats are more pressing than external ones. However, internal threats arise as a result of the lack of sound information security behaviour amongst employees and users.

Research by Safa *et al*. (2016) on information security awareness showed that awareness of security had a significant effect on employees' attitudes towards compliance. The study identified information security awareness as a key factor in employees' compliance with information security policy. Tsohou *et al*. (2015) examined the impact of end-user security awareness training on employees' compliance behaviour and found that training employees increased their knowledge of security. Ineffective or inappropriate security decisions may arise

where there is ignorance of security threats. Hence, this study posits that security awareness will affect the behavioural intention of employees and in turn, their compliance with ISSPs. It further hypothesises that employee behavioural intention will mediate the relationship between awareness of information security and ISSsPs.

3.6.7 Behavioural Intention to Comply

This is a human behavioural construct which intermediates actual behaviour by highlighting the intention to act. In this study, it is operationalised as employees' explicit intention to comply with ISSsPs. Consequently, Kim *et al*. (2014) investigated the factors that influence an individual's intention (student) to use information security technologies. The authors found that a user's attitude will determine their intention to use security measures to protect information. Kim and Park (2013) employed the Protection Motivation Theory (PMT) to test and measure users' information security behaviour. The results also showed that a user's attitude to security has a significant impact on individual behavioural intention to comply with security measures. Furthermore, behavioural intention has to do with one's willingness to use information security, which requires some understanding on the part of the user on how they can protect their information from threats or abuse.

3.7 Hypotheses

Based on the theoretical foundation, the reviewed literature and the study's research questions and objectives, the hypotheses are categorised into two parts: direct and indirect influence. The hypotheses were developed to test the direct and indirect influence of motivational factors on employee behavioural intention to comply with ISSsPs. The **direct** hypotheses are as follows:

H1: Normative beliefs influence employees' behavioural intention to comply with ISSsPs.

H2: Awareness of information security threats influences employees' behavioural intention to comply.

H3: Perceived effectiveness of information security compliance influences employees' behavioural intention to comply.

H4: Perception biases influence employees' behavioural intention to comply.

H5: Certainty of detection influences employees' behavioural intention to comply with ISSsPs.

H6: Severity of penalties will influence employees' behavioural intention to comply with ISSsPs.

The remaining hypotheses were formulated to show the mediating effect of the intention to comply and the behavioural factors. The following are the **indirect** (mediating) hypotheses that are tested:

H7: Employees' behavioural intention to comply mediates the relationship between the severity of penalties and ISSsPs compliance.

H8: Employees' behavioural intention to comply mediates the relationship between certainty of detection and ISSsPs compliance.

H9: Employees' behavioural intention to comply mediates the relationship between normative beliefs and ISSsPs compliance.

H10: Employees' behavioural intention to comply mediates the relationship between awareness of information security threats and perceived effectiveness of ISSsPs compliance.

H11: Employees' behavioural intention to comply mediates the relationship between the perceived effectiveness of ISSsPs and ISSsPs compliance.

H12: Employees' behavioural intention to comply mediates the relationship between perception biases and ISSsPs compliance.

In order to understand the relationship between these hypotheses, the conceptual framework and the research questions, the next paragraph discusses this.

As shown in the conceptual framework in Figure 3.6, the dependent variable of this study is ISSsPs compliance. With due attention to FISMA, HIPAA, SOX, ISO/IEC 17799 and GLBA (the international standard codes and policies considered for this study), questionnaire items were designed to assess the individual banks' compliance rate. This answers the first research question.

Moreover, FISMA, HIPAA, SOX, 1SO/IEC 17799 and GLBA were selected due to the fact that these standards cover major security aspects of the banking sector's services and also address the study's main concern. Information security breach dimensions were also designed

into questionnaire items to assess the rate at which the banks have experienced them. Appropriate statistical techniques were subsequently used to test the hypotheses, specifically the hypothesised influence of compliance rates on experiences of information security breaches. This answers the second research question.

The study's conceptual framework includes a list of employees' behavioural factors, which are referred to as motivational factors. This is based on a review of related studies. The direction (positive or negative) and magnitude (significant or insignificant) of the influence of the highlighted factors on both employees' behavioural intention to comply and actual compliance with ISSsPs were then investigated. Employees' intention to comply is the mediating variable of this study. A mediating variable is a pathway towards the actualisation of the dependent variable. This answers the third research question. The interpretation of the data collected to answer the earlier research questions is contextualised within the body of knowledge that informed this study. Debates and findings presented in previous empirical studies are drawn up to identify the strategies required by developing a framework which reduces experiences of cyber theft and fraud in Nigerian banks. This answers the fourth research question.

3.8 Empirical and Theoretical Review of Past Studies on Information Security

A review of previous studies on information security was conducted in order to identify the gaps in the literature. According to Siponen, Mahmood and Pahnila (2014), the key threat to information security emanates from employees who do not comply with the organisation's information security policies. Choi *et al*. (2018) noted that information security is designed to protect personal and organisational assets and disallow unauthorised access. It includes measures to safeguard data from unlawful disclosure, modification, disruption and complete destruction. An extensive review of the literature by Choi (2016) suggested that information security research can be grouped into four categories: interpretive, radical humanist, functionalist and radical structuralism. The author suggested that in order to understand information security-related issues, a socio-organisational theory should be employed because most technology related to information security issues is maintained, signed for and used by (human) employees within the organisation.

According to Sinha *et al*. (2019), information security involves safeguarding the confidentiality, integrity and availability of information, while Soomro *et al*. (2016) conducted

a study in order to develop a model for managerial perceptions of information risk and how they compare with existing information security policies. A study by USA 530 Enterprises found that 90% of organisations had suffered information security breaches and 75% had experienced business difficulties due to such breaches, with losses estimated at around $201 million. As technological solutions are not sufficient to ensure information security, users must also be brought on board. This view is widely held in the literature. Evans *et al*. (2019) note that the human factor is the weakest link in information security. It is for this reason that Jalali *et al*. (2019) emphasised that employee compliance with ISSsPs is very important. Besides, Sharma and Warkentin (2019) investigated how perceptions of information security amongst employees in the banking sector influence their attitudes towards such security. The 602 respondents were asked to evaluate one of the 21 common threats to information security. The results show that individual experiences control employee perceptions of information security in terms of the exploration of human factors for combating insider threats. The authors developed a framework to categorise information security requirements into different control groups and then measure the level of information security in an organisation. The authors also proposed a method which can be combined with other measures to provide an indication of overall information security and to assist information security personnel in identifying appropriate strategies. It can gauge the effect of a single control measure on the total security system. Pathari and Sonar (2013) suggested that information security is slowly but steadily becoming an integral part of all operations, rather than being a spin-off.

Information security requires that employees comply with ISSsPs, which can be achieved through motivation and persuasion. Moreover, Jalali *et al*. (2019) investigated why employees still click on phishing links after receiving training. They explored the factors that influence information security policy compliance, using the theory of planned behaviour (TPB) and trust theories. Protection motivation theory was not considered by the author, combining (TPB) and (PMT) gives a precise and accurate explanation in predicting the behavioural change.

Information security encompasses the use of physical and logical data access control to ensure the proper use of data and prohibit unauthorised or accidental modification, destruction, disclosure, loss or access to automated or manual records and files and other information assets. However, this definition does not address the measures that should be taken to ensure such security as well as maintain it. Ferreira *et al*. (2019) stated that where businesses are hyper-

connected, organisations are under serious and constant threat from users. The authors' empirical study investigated information security planning at different strategic levels and stages of threat. They also sought to identify the values that enhance information security programmes. The results suggest that information security governance is crucial to successful information security planning. The authors added that information security technology can be used to address information security as a total enterprise issue. Finally, Ferreira *et al*. (2019) concluded that information security should be integrated with strategy formulation and that the former is one of the major responsibilities of top managers.

Yeh and Chang's (2007) empirical study examined the gap between managers' perceptions of information security threats and security counter-measures adopted by the IT section of an organisation. The results showed that implementation did not affect managers' perceptions of threats, and that the countermeasures implemented could not be measured with the severity of the perceived threats to the organisation. The difference between the internal and external functions of information security systems are very clear- the internal functions focus mainly on technical aspects, while external functions revolve around managerial and operating security. AlHogail (2015) investigated the concepts that needed to be considered when designing information security policies for a university and suggested vital strategies that should be adopted. First amongst them is dealing with information security threats at the same time as risk management and developing a sound platform for information security policy. The second strategy relates to authentication access control (incorporating cryptography) and backs it up with the management of information security. In addition, Singh, Pandiya and Sing (2020) examined potential threats to the banking sector, as well as typical information assets. They suggested a compressive information security framework to protect banks' information systems. They also recommended the adoption of information security standards like FFIEC, COBIT, ISO 27002 and PCI for data security. Islam (2020) investigated the primary threats to information security in the banking sector and designed a conceptual framework to address them. The author suggested the need for regular (daily) checks of all business transactions and updating the information system which houses banking information and customer data. The study also suggests changes to IT policies in order to address cybercrime.

Jassal and Sahgal (2013) examined the security and technology standards designed to eliminate banking fraud and analysed the Industrial Credit and Investment Corporation of India's (ICICI)

banking information security, where the results show that cybercriminals have many ways to access institutions' financial systems as well as bank customers' accounts. In addition, Al-Alamimi (2011) noted that most banks in Saudi Arabia are more concerned with external than internal threats. As a result, bank employees feel more protected from external threats. In relation to Mwashiuya and Mbamba (2020), the relationship between information technologies in financial and banking institutions, as well as technology risk factors, were examined. The authors advised that information security should be given high priority and that new technologies should be adopted to carry out daily transactions.

An organisation's information security depends absolutely on employee compliance with information security policies. The authors note that information users harbour the notion that technology can solve the problems of information insecurity, while Safianu, Twum and Hayfron-Acquah (2016) agreed that this will not always yield satisfactory results as the human factor has a significant effect on computer security. They note that individual differences, cognitive abilities and personality traits have a profound influence on employee compliance with information security policies, suggesting that employee behaviour influences the organisational culture and information security environment.

Von Solms and Niekerk (2013) examined the gap between information security and cybercrime. They are of the view that while information security and cybercrime are somewhat related, they are not similar as the general definition of information security includes the requirements of integrity, availability and confidentiality, while cybercrime embraces additional dimensions beyond information security issues, such as humans in their different capacities and society at large. When it comes to information security, the harm done to information is always indirect. Organisational collaboration is thus essential to protect an organisation from information security threats and cybercrime.

Moody *et al*. (2019) investigated the factors that motivate employees to comply with information security policies in relation to technological resources and information from intruders. The study focused on information security awareness and perceived fairness. Using partial least squares for data analysis, the results suggest that information security awareness and perceived fairness positively influence attitude, which in turn influences intention to comply. Information security awareness has an indirect influence on perceived attitude because

it positively influences perceived fairness. The authors concluded that the role of employee information security awareness cannot be over-emphasised.

Numerous studies have been conducted on the lack of employee participation in information security at the planning stage, leading to poor levels of compliance with subsequent policies (Chua *et al*., 2018). However, such compliance could increase employee satisfaction. Herath and Rao (2009) add that a lack of motivation is one of the major factors hindering employee involvement in planning information security standards and policies.

The human aspect is of primary concern in ensuring the protection of both organisational and individual information and assets because people have a direct link with such information and assets, hence it is their responsibility to protect them. This can be achieved through compliance with the rules and standards (AlHogail, 2015). Unequivocally, employee involvement should not be neglected.

Many studies have noted the deterrent impact of sanctions and the effect of incentives in encouraging employees to comply with ISSsPs. Malimage *et al*. (2019) identified the factors that influence employee compliance with information security policies. ISSsPs address information security and provide a precise definition of what the organisation should focus on and how the mechanisms should be devised. Organisations should make ISSsPs available to their employees to serve as a guideline to protect information (Bulgurcu *et al*., 2010). Based on the literature reviewed,this study identified gaps that needed to be filled.

3.9 Gaps Filled by the Study

The literature review revealed that a clear theoretical explanation has not been provided of the intrinsic and extrinsic factors which influence employees' behavioural intention to comply and compliance with ISSsPs. The gaps filled by this study are:

a) the lack of studies on Nigerian banks' rate of compliance with information security in order to establish the extent of their compliance;
b) the lack of empirical studies on the influence of employees' motivational factors on Nigerian banks' compliance with ISSsPs; and
c) the lack of theoretical explanations of the hypothetical mediating role of employees' intention to comply in the actualisation of Nigerian banks' compliance with ISSsPs.

3.10 Chapter Summary

This chapter presented and discussed a number of theories on human behaviour. Three of these theories were selected for this study, viz., the TPB, theory of self-efficacy and PMT. Factors such as severity of penalty; certainty of detection; normative beliefs; perceived effectiveness of ISSsPs compliance; perception bias; and awareness of security threat were identified as influencing employees' behavioural intention to comply with ISSsPs, which in turn affects their actual compliance with ISSsPs.

This chapter also reviewed relevant literature to highlight the gaps addressed by this study; the operationalization of the variables investigated; and the justification for the proposed research model. It discussed employee behavioural factors which are antecedents to organisational compliance with ISSsPs, as well as employees' behavioural intention to comply. Finally, the proposed research framework that highlights the conceptual relationship between the antecedent variables, the mediating variable and dependent variable, as well as the factors that generally influence employees' compliance, especially the human factors, was presented.

Chapter Four, which follows, discusses the method adopted to conduct this research in detail, focusing on the research design, the data collection survey instrument and sampling and data analysis. Section 1.8 presented some level of research design but not in detail, as the purpose was to allow the reader to familiarise themselves with the method adopted in this study.

CHAPTER FOUR
RESEARCH METHODS

4.1 Introduction

This chapter discusses the research design adopted to achieve the research objectives and answer the research questions. It presents the methodological framework which outlines the linkages between the theories, research constructs and research objectives, as well as the method adopted to achieve each of the objectives. The survey instrument design, sampling and data collection and data analysis are also discussed. The approaches adopted in each of the research phases are highlighted and justified.

4.2 Research Approach

A research approach, also referred to as research methodology in some studies (Bell *et al*., 2018), is the overall approach in the research process, from the theoretical underpinnings to the collection and analysis of the data (Roth *et al*., 2020). It is also defined as the general approach that entails identifying the case(s) to study and choosing the appropriate data collection and analysis methods (Silverman, 2019), the way in which research is conducted, as well as how this relates to the knowledge that results from the research (Anderson *et al*., 2019). According to Peffers *et al*. (2020), a research methodology is a structured way of making an inquiry by employing acceptable scientific methods to solve problems and create new knowledge. It is a structured procedure to investigate the research problem identified, involving data collection and analysis (Ofusori, 2019).

Research approaches are broadly classified into quantitative, qualitative and mixed research methods in which both quantitative and qualitative methods are employed. The following sub-sections elaborate on the different research approaches.

4.2.1 Quantitative vs. Qualitative Research

Bell *et al*. (2018) state that qualitative and quantitative approaches are the two main research methods. The third, which is a combination of both, is known as the mixed method approach. The main difference is in the nature of the data collected and the manner in which it is gathered. The choice of research approach is determined by the research questions (Yoko *et al*., 2020).

A quantitative study investigates a social problem through an empirical testing of theories and a statistical analysis of data. On the other hand, a qualitative study aims to understand a social phenomenon by building a comprehensive theory. Therefore, the distinction between

quantitative and qualitative approaches is based on the nature of the data (numerical or non-numerical), as well as deeper differences in their philosophical foundations and the paradigm employed- Deductive vs. Inductive Research (Bell *et al*., 2018).

Collis and Hussey (2003) state that research can also be classified based on whether the researcher moves from the general to the specific or vice versa. A deductive study is one in which the researcher develops a theoretical structure and then tests it empirically. The aim is to deduce a particular instance from general inferences (Dissanayake, 2015). In inductive studies, the reverse occurs, and a theory is generated from observations (moving from the specific to the general) (Bell *et al*., 2019). This implies that quantitative studies are generally deductive, while qualitative ones are inductive.

4.2.2 Cross Sectional Vs. Longitudinal

According to Saunders *et al*. (2012), research is cross-sectional when it is taken at a particular time. In such studies, information is collected only once or at a single point in time (Diehl *et al*., 2020). However, it could take days, weeks or even months to collect the required data (Schuurman, 2020). Equally, Saunders *et al*. (2012) added that cross-sectional research is used when researchers have limited time or resources. On the other hand, longitudinal studies can be more like a "diary" and are used to represent events over a given period of time. In such studies, the researcher aims to collect the data about a certain phenomenon over a period of time or at more than one point in time (Dolnicar, 2020).

.

4.2.3 Research Paradigm

A paradigm is "a cluster of beliefs and dictates which influence, what should be studied, how research should be done and how results should be interpreted" (Yuan *et al*., 2020). Silverman (2005) defines a paradigm as a general framework to examine reality. Additionally, Sarantakos (2013) argues that two paradigms guide business research, namely empiricist (objectivism) and humanistic (subjectivism). In addition, Saunders (2012) states that in positivist research, researchers employ a deductive approach to identify causal relationships; collect quantitative data from a large sample; and use a highly structured methodology to enable them to replicate their findings.

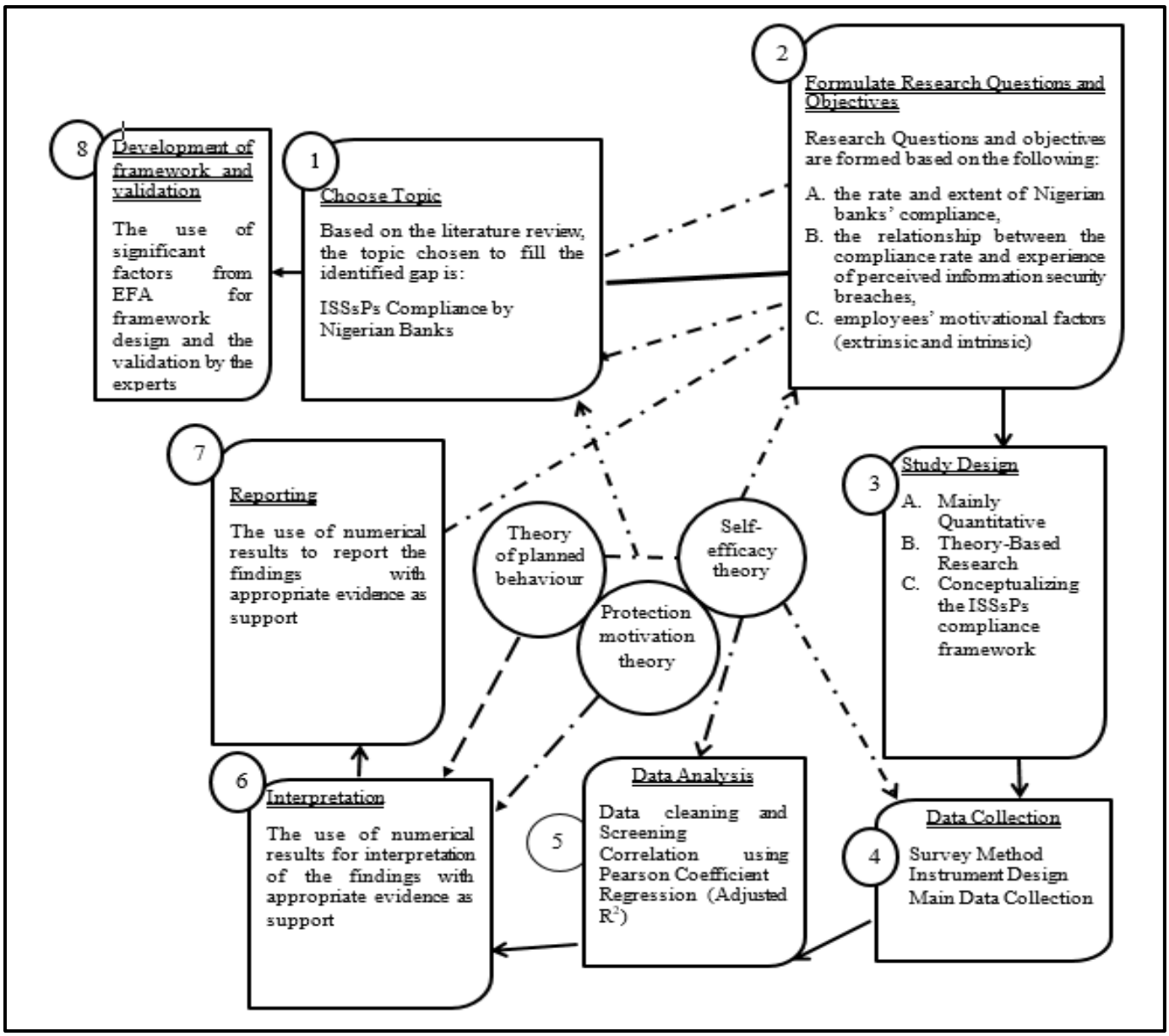


Figure 4.1: Research Methodological Framework (Source: Author's own)

Positivism answers deterministic research questions through testing hypotheses (Zikmund *et al*., 2019). Research activities follow seven phases, revolving round the study's main theory. The research paradigm shows the steps taken to achieve the study's purpose. Generally, these include formulating the research topic; framing the research questions and objectives; designing the study; data collection; data analysis; and interpretation and reporting. Each step is followed in strict order in order to achieve the research objectives.

As discussed in Chapter Three, this study is guided by its underpinning theories and associated theories. Figure 4.1 presents the research methodological framework.

4.2.4 Stages and Steps in the Methodological Framework

The *first stage* of the research, as presented in Figure 4.1, was the choosing of the topic, which is a crucial step in any study. The topic was selected based on the problems identified. A thorough review of literature was conducted in order to identify the gaps. The researcher used Google search to identify studies on information security and standards. It was found that only a few studies have been undertaken on information security standards and policies compliance, particularly in the Nigerian context. The study combined standards and policies to address compliance with information security in the Nigerian banking sector (Nawale, 2020) .

.

The *second stage* of the research, as presented in Figure 4.2, addressed the research objectives and questions. These were formulated based on the following: the rate and extent of Nigerian banks' compliance; the influence of compliance rates on experiences of perceived information security breaches; and employees' motivational factors.

The *third stage* in this research was a conceptualisation of ISSsPs into the conceptual framework, which consists of certain elements (severity of penalty; certainty of detection; normative beliefs; perceived effectiveness of ISSsPs; awareness of information security threats; and perception biases) which are used to measure the change in employees' behaviour (ISSsPs).

In *stage four*, three theories were integrated into the framework, i.e., the TPB, self-efficacy theory and the PMT.

The *fifth stage* in the research framework was data collection, as seen in Figure 4.3. This involved designing the survey instrument and data collection.

Stage six involves an interpretation of the results based on the data collected and the data analysis. Numerical results were employed for the interpretation of the findings, with appropriate evidence.

The *final stage* in the framework is reporting the outcomes of the data analysis.

The study employed a quantitative research approach. A deductive approach was adopted, which allowed for empirical testing of the hypotheses and for the results to be generalised. A

cross-sectional survey method was employed to collect the right amount of data from a sizeable population in an economical manner. Therefore, this research adopted a positivistic research paradigm and a quantitative research framework, with its conceptual framework constructed from related theories to guide the entire research process.

A quantitative research approach involves quantitative data which are expressed in numerical and statistical ways and analysed and measured using statistical methods (Marchingo *et al*., 2020). The quantitative research design allows the researcher to analyse respondents' behaviour (Lakshman *et al*., 2000). Moreover, Smith *et al*. (2012) stated that a quantitative research design can validate a study's conclusions by verifying the established concepts and proving or disproving a proposed concept. Peffers *et al*. (2020) added that a quantitative research design can produce consistent results when used with a descriptive research design. Several researchers have also identified the quantitative research design as the most suitable approach to investigate individual opinions, as well as the motives behind respondents' actions, behaviour and attitudes.

This study firstly critically reviewed related past studies to identify, conceptualise and operationalize employee behavioural constructs that can affect employees' intention to comply, as well as their eventual compliance with ISSsPs. Secondly, using the theoretical underpinnings of the PMT, TPB and self-efficacy theory, and based on related past studies, a survey instrument was designed and administered to a sample of Nigerian bank employees. Thirdly, the data collected was analysed using appropriate statistical techniques and tools to provide answers to the research questions. Data cleansing was undertaken during the data analysis process in order to achieve validity and reliability. Further details are provided in the next section.

4.3 Data Collection and Analysis

Data collection methods are an integral part of any research design in order to provide answers to the research questions. This section discusses the type of data used in this study, the survey instrument design, the sampling strategy, data analysis, interpretation and reporting.

4.2.1 Types of Data: Primary and Secondary Data

According to Ghauri *et al*. (2020), research data can either be primary or secondary. Secondary data are data from journal articles, books and online or offline repositories. The importance of secondary data lies in the fact that it sharpens the focus of a research study and also enables gaps to be identified in the body of knowledge in a particular field. Furthermore, it serves as a theoretical base to familiarise the reader with credible sources of academic work underpinning the framework of a thesis.

Primary data refers to data collected directly from respondents. This study employed a survey questionnaire that drew on supporting theories and past related studies to identify the variables. According to Apuke (2017), there is a relationship between the data collection method employed and the quality of the results obtained. Therefore, the appropriateness of the data collection method must be adequately considered. In this study, data were collected from the respondents by means of a questionnaire using a direct approach, i.e., the researcher personally administered it in order to ensure a higher response rate. A questionnaire is a results-oriented survey technique, especially when respondents' opinions are involved.

Data collection generally involves two phases, namely the pilot phase and the main study. The pilot phase enables the researcher to identify errors for correction prior to the main study (Creswell, 2014). This study also included a presenting phase whereby a research consultant was employed for content validity of the instrument (Pallant, 2011) and the comments provided were used to improve the questionnaire. The design of the questionnaire, also known as the survey instrument, is explained in the next sub-section.

4.2.2 The Research Choices

Creswell and Poth (2017) and Bowen *et al*. (2017) categorised research choices into three, namely quantitative, qualitative and mixed methods. The quantitative approach is characterized by the use of numbers and closed-ended questions, as opposed to the use of words and open-ended questions or interviews on which the qualitative approach centres. In this study, higher priority was given to quantitative data: through this, generalization of the study findings can be proposed.

Lastly, it creates an avenue for a separate analysis of quantitative data, which was later integrated at the interpretation stage. Ofusori (2019) noted that the methods enable quantitative (numerical) data to be collected and analysed concurrently, depending on the study's research questions and objectives, as well as the problem statement (Yoko *et al*., 2020)

In the Nigerian banking sector, it is important to note that different respondents and organisations may have different practices, views and experiences and thus applied these when answering the questions. Thus, a Quantitative method was considered more suitable as it falls in line with the philosophical worldview of the study (Creswell, 2014). In this study, two phases are considered: the first one is an identification of the problems which led to the development of the framework evaluation. For the first phase, a quantitative approach was used to gather information regarding banks' practices, which covers the type of standards employed, how regularly they review their standards. The question sought to determine the banks' practice and their experience regarding information security issues. The second section of the question is regarding the motivation factors, otherwise referred to as employees' behavioural factors. The questions are designed on a scale, which is used for the model.

4.2.3 Survey Instrument Design

The questionnaire was designed based on the supporting theories and past related studies that were adapted to meet the study's objectives, as described in Chapter Two of this thesis. Arguments from the supporting literature were also taken into account. Each of the variables investigated in this study is a continuous variable. These are severity of penalty; certainty of detection; normative beliefs; peer behaviour; perceived effectiveness of ISS compliance; perception bias; and awareness of information security threats. The mediating variable is employee behavioural intention to comply, while perceived ISSsPs compliance is the dependent variable.

The items of the instrument were designed in such a way that the constructs' dimensions were reflected and adequately measured. This ensures a relationship between the conceptual explanations of the constructs and the items in the instrument (Zikmund, Babin, Carr and Griffin, 2010). The items were designed to measure bank employees' behavioural intention to comply; perceived ISSsPs compliance; and the hypothesised antecedent variables.

Data collected from the survey questionnaire was quantified using a Likert scale. According to Chevalier *et al*. (2020), the Likert scale is used to collect respondents' responses to questions in the form of numerical values. This study used a 7-point Likert scale because it strikes a good balance between points of discrimination without too many response options (Kandasamy *et al*. 2020). Therefore, the 7-point Likert scale is used to address the issues concerning the questionnaire.

4.2.3.1 Severity of Penalty

This variable measured how employees perceived the severity of the penalty meted out to anyone caught violating the organisation's security policies, as well as how well-enforced these security policies were in terms of deterring and punitive measures (Herath and Rao, 2009). The six items were adapted from Herath and Rao (2009). Table 4.1 presents the items of the severity of penalty variable and the respective item coding for data analysis.

Table 4.1: Severity of Penalty

Code	Items
SOP 01	Employees caught violating security policies are appropriately corrected.
SOP 02	Information security policies are enforced by punishing employees that break them.
SOP 03	Serial information security offenders among the employees are appropriately disciplined.
SOP 04	Employees who repeatedly break security rules can lose their jobs.
SOP 05	If I were caught violating organisation information security policies, I would be severely punished.
SOP 06	My employer takes strict action against violation of information security policy.

4.2.3.2 Certainty of Detection

This variable measured how employees perceived the efficacy of the organisation's monitoring mechanism with respect to the early detection and awareness of security policy violations on the part of either internal (employee) or external (virus, or any form of attack) agencies (Vance *et al*., 2012; Johnston and Warkentin, 2010).

Equally, certainty of detection can be conceptualised as an inverse of the severity of the security threat (Ng, 2008). The five items were adapted from Herath and Rao (2009). Consequently, Table 4.2 presents the items of the certainty of detection variable, as well as the respective item coding for data analysis.

Table 4.2: Certainty of Detection

Code	Items
COD 01	My computer practices are properly monitored for policy violations.
COD 02	If I violate organisation security policies, I will most likely be caught.
COD 03	My computer is monitored for security threat exposure.
COD 04	I am assessed for information security compliance.
COD 05	My computer is routinely checked for security threats.

4.2.3.3 Normative Beliefs

This variable measured the extent to which employees act on the basis of what other employees expect of them, or what the organisational standard/norm expects of them (Kaymaz, 2020). It is otherwise conceptualised as peer pressure (Herath and Rao, 2009). This measures how peers (in this case, co-employees) directly or indirectly influence employees' security-adhering actions. The five items for this variable were adapted from Pahnila *et al*. (2007). Table 4.3 presents the items of the normative beliefs variable and the respective item coding for data analysis.

Table 4.3: Normative Beliefs

Code	Items
NOB 01	It is important to me for my co-workers to see me as an ethical person.
NOB 02	My co-workers believe I should comply with information security policy standards.
NOB 03	I comply with inform security standards because my superior assesses my work.
NOB 04	My co-workers believe it is important to comply with information security policy standards.
NOB 05	To my knowledge, most employees comply with the organisation's IS security policies.

4.2.3.4 Perceived effectiveness of ISSsPs Policies Compliance

This variable measured how employees perceive the effectiveness of complying with ISS policies in view of the benefits attached (Cheng *et al*., 2013). The six items for the variable were adapted from Said *et al*. (2013). Table 4.4 presents the items of the perceived effectiveness of the ISS policy compliance variable and the respective item coding for data analysis.

Table 4.4: Perceived Effectiveness of ISSsPs Policies Compliance

Code	Items
PEF 01	Our information security policy is effective in achieving our organisational goals for information security.
PEF 02	Our information security policy helps to accomplish the information security objectives.
PEF 03	Our information security policy keeps the risk at a minimum.
PEF 04	Compliance with the requirements of the information security policy, reduces security risks.
PEF 05	Compliance with the requirements of the information security policy secures our infrastructure.
PEF 06	Overall, the information security policy is effective in securing information at this organisation.

4.2.3.5. Awareness of Information Security Threats

This variable measured the extent of employees' awareness of information security threats through self-education, organisational programmes and on-the-job training (Gundu and Flowerday, 2013; Moores, 2013). Moreover, the seven items were adapted from Gundu and Flowerday (2013). Table 4.5 presents the items for the awareness of information security threats variable and the item coding for data analysis.

Table 4.5: Items of Awareness of Information Security Threats

Code	Items
STA 01	I clearly understand the implications of violating security policies.
STA 02	I have received education about information security threats.
STA 03	Information regarding security threats has been communicated to me.
STA 04	I know about a continuous awareness programme on general information security threats.
STA 05	Information security training was included as part of my orientation.
STA 06	Information security policies are discussed during my annual evaluation.
STA 07	My supervisor updates me on changes to information security procedures.

4.2.3.6 Perception Bias

This variable measured the correctness, or otherwise, of the employees' perceptions and understanding of the security issues at hand, as well as their judgement of the action to be taken to avert or correct such a security crisis (Herath *et al*., 2014). The eight items were adapted from Herath (2014). Table 4.6 presents the items for the perception biases variable and the respective item coding for data analysis.

Table 4.6: Items of Perception Bias

Code	Items
PCB 01	In case of an information security threat, I always act swiftly no matter the severity of the threat.
PCB 02	The measures in place to counteract information security threats are suitable and work successfully.
PCB 03	The measures we use to counteract information security threats can successfully deal with the most complex of threats.
PCB 04	The security-resisting mechanisms in place are successful in counteracting most threats that we experience.
PCB 05	If I am unsure about a possible security threat, I prefer to take swift preventative measures rather than ignore it and must fix it after it has happened.
PCB 06	The organisation sets high standards for the protection of its information assets.
PCB 07	Overall, compliance of the Information Security Policy at this organisation is good.
PCB 08	The policies in place regarding information security are adequate to address security threats.

4.2.3.7 Behavioural Intention to Comply

These variable measured employees' behavioural tendency to comply with ISS policies (Gundu and Flowerday, 2013; Lee *et al*., 2016). It was hypothesised as a consequent variable to the listed antecedent variables and as the antecedent variable to ISSsPs compliance. It was therefore tested as a mediating variable.

Table 4.7: Employees' Behavioural Intention to Comply Items

Code	Items
EBI 01	In my daily work, I try to protect information and technology resources according to the requirements of the ISSsPs of my organisation.
EBI 02	When I use information technology, I try to carry out my responsibilities as prescribed in the ISSsPs in order to ensure the security of the information I am working with.
EBI 03	When performing my daily work, I try to comply with information security procedures.
EBI 04	I tend to ignore information security procedures that I think are not necessary.
EBI 05	My intention is to follow my organisational security policies wherever possible.
EBI 06	I intend to comply with information security policies.

The six items were adapted from Gundu and Flowerday (2013). Table 4.7 presents the items for the employees' behavioural intention to comply variable and the respective item coding for data analysis.

4.2.3.8 Perceived ISSsPs Compliance

This variable measured the extent and rate at which the ISSsPs is complied with by the organisation, as assessed by employees (Johnston and Warkentin, 2010). The five items were adapted from Herath and Rao (2009). Table 4.8 presents the items for the ISSsPs compliance variables and the respective item coding for data analysis.

Apart from the items designed for each of the variables investigated in this study, other items were designed to address further components of the research objectives. These are the ISS policies compliance rate and information security breach experiences.

Table 4.8: ISSsPs Compliance Items

Code	Items
ISS 01	My organisation's information security policy is consistently updated on a periodic basis.
ISS 02	My organisation's information security policy evolves as technology changes.
ISS 03	There is a review system for our information security policy standard in my organisation.
ISS 04	My organisation complies with major ISS policies.
ISS 05	ISS policy compliance is part of the organisation's core values.

4.2.3.9 ISSsPs Compliance Rate

This is a non-continuous measurement of ISSsPs compliance. It measures the rate in terms of how often the organisation reviews its security policies; the type of ISSsPs it subscribes to; and the frequency of adopting new ISSsPs. The designed responses to the items ISR 01, 02 and 03 are presented in Tables 4.9, 4.10 and 4.11 respectively.

ISR 01: How often does your organisation review its ISSs Policies (ISSsPs) compliance?

Table 4.9: Responses to Item ISR 01

Less Often than Once A Year	At least Once A Year	At Least Once Every 6 Months	At Least Once Every Quarter	At Least Once A Month

ISR 02: Which of the following international ISSsPs does your organisation subscribe to? (Tick ALL that apply)?

Table 4.10: Responses to Item ISR 02

FISMA	
HIPAA	
SOX	
ISO/IEC 17799	
GLBA	
Other: Specify	

ISR 03: When last did your organisation adopt a new ISS Policy (ISSP)?

Table 4.11: Responses to Item ISR 03

More than a year ago	Between 6 months and a year ago	Between 3 and 6 months ago	In the last 3 months

4.2.3.11 Information Security Breach Experience Dimension

This is a non-continuous measurement of information security breach experiences. It measures the rate of information security breaches in terms of how often the organisation experiences them; the type of ISS policy that is most prone to security compromise; and the last record of a security breach. The designed responses to the items ISB 01, 02 and 03 are presented in Tables 4.12, 4.13 and 4.14, respectively.

ISB 01: How often does your organisation experience information security breaches?

Table 4.12: Responses to Item ISB 01

Less Often than Once A Year	At least Once A Year	At Least Once Every 6 Months	At Least Once Every Quarter	At Least Once A Month

ISB 02: Which of the following international ISSPs, in your experience, successfully prevent an information security breach? (Tick ALL that apply).

Table 4.13: Responses to Item ISB 02

FISMA	HIPAA	SOX	ISO/IEC 17799	GLBA	Other: Specify

ISB 03: When last did your organisation successfully avert a pending information security breach?

Table 4.14: Responses to Item ISB 03

Never	More than a year ago	Between 6 months and a year ago	Between 3 and 6 months ago	In the last 3 months

4.4 Population, Sample Size and Sampling Strategy

This study was conducted in the Western part of Nigeria, which has a large population and is the centre of corporate activity in the country. The headquarters of all Nigerian banks are located in this part of the country. The selection of the study site meant that the corporate offices of the chosen banks could be visited and the questionnaire successfully administered. The population size for this study consisted of 10 banks, according to Ofusori (20190, that can be categorised under three groups, namely first-generation, second-generation and third-generation banks.

The first-generation banks are First Bank and Union Bank which were established between 1952 and 1985. The second-generation are the new generation banks, mostly embellished in 2004 during the time banks were experiencing financial turbulence, where some of the banks merged. These are Zenith Bank, Access Bank, Wema Bank, Guarantee Trust Banks, Skye Bank and City Bank. Third-generation banks are micro finance-banks and others like Heroes Bank and FTC Bank. New banks were established between 2008 and 2015.One bank from each of these groups (making three banks in total) was purposively chosen to represent the study population because:

a) they are amongst the banks that adopted ISS related to FISMA, HIPAA, SOX and ISO/IEC 17799;

b) they cut across all three categories in the western part of Nigeria, thus enabling a level of generalizability; and
c) according to Glaser's sampling dicta (Glaser, 1967), they have the tendency of maximizing possibilities of substantive data that foster data analysis. Therefore, some banks were selected on the basis of this dicta. Furthermore, the ethical regulations guiding research at UKZN stipulate that only organisations with open ethical regulations can be used. Although seven banks were investigated for the study, only three banks agreed to participate in the study.

The participating banks, who requested to remain anonymous, are references using pseudonyms. The request was declared when seeking permission to conduct the study for both the primary data and the data used for framework validation

The banks selected were Bank A, Bank B and Bank C. These banks were purposively selected in line with Glaser's dicta (Glaser, 1998) that sites should have: (i) the tendencies of maximizing possibilities; (ii) the capacity to enhance and refine the scope of methodological inquiry; and (iii) the proclivity for increasing representativeness through variation abstraction. The purposively selected banks are also the most patronised and have the highest capital reserves amongst commercial banks. The three selected banks have their Head Offices at the location of the case study.

The sampling strategy employed was representative sampling with purposive intent. This is also referred to as purposive sampling. The participant selection was based on the judgement of the employees: (i) Having in-depth knowledge and expertise of the concepts of information security; (ii) Having recent hands-on experience of policies and standards in relation to information security; and (iii) Having extensive involvement in information security management.

Moreover, serious consideration was given to the willingness of the experts to participate in the validation exercise. The data was collected from employees of the three banking institutions that provided the required ethical clearance. The unit of analysis is therefore an individual (bank employee) (Babbie, 2010; Creswell, 2009; Neuman, 2007). Table 4.15 shows the number of employees in each of the three banks, as well as the sample drawn according to Morgan's

theory of determining a sample size from a given population (Krejie & Morgan, 1970). The sample size that corresponds to the total workforce of 17,916 for the three organisations is 370.

Table 4.15: Sample Size Drawn from the Employees

Name of Bank	No. of Employees in 2015	Sample Size
First Bank plc	7,616	370
GTBank	10,000	
FCT Bank	300	
Total	17,916	

The sample size was proportionate to each of the banks based on their employee strength. It was calculated using SI as individual sample size; PI individual population size; and TP total population, i.e. 17,916. Table 4.16 shows the sampling frame for questionnaire administration. The individual sample sizes served as a guide for the questionnaire administration for the three banks so that each bank was treated proportionately. The participants selected within the banks are e employees with specific expertise who have knowledge about information security.

Table 4.16: Sampling Frame for Questionnaire Administration

No	Name of Bank	Number of Employees (Individual Population Size; PI)	Individual Sample Size (SI, where 370) IS $\frac{IP}{TP} * 370$
1	First Bank	7,616	157
2	GTBank	10,000	207
3	FCT Bank	300	6
	Total	17,1916	370

4.5 Data Analysis, Interpretation and Reporting

The data collected were analysed using different statistical techniques, which were determined by the research questions and the hypotheses tested. Data analysis mainly relied on SPSS

software. For item reliability, the values of the Cronbach Alpha coefficient were used to determine the individual item reliability, internal consistency reliability, convergent validity and discriminant validity (Pallant, 2011).

A validity test involves testing the strength of the measurement, while a reliability test seeks to test for the internal consistency of an instrument. Reliability and validity are data validation techniques. Data validation is done in two main ways: content validity and construct validity. The Cronbach's Alpha level is interpreted to determine the reliability of the items of each variable construct, with an acceptable value of 0.6 or above. Each question of the instrument items was re-framed and duplicated using different words to examine if there could be any variation in understanding or misunderstanding of the responses to any of the questions. The process of content validity ensured the objectivity and authenticity of the research.

Descriptive and inferential statistics were employed. Descriptive statistics includesthe frequency distribution of the sample and the opinions represented. Inferential statistics include correlation and regression, as well as bootstrapping to establish the relationship between variables, test for causal effect and test for mediating effect, respectively. The inferential statistics were conducted using SPSS to find the Pearson Correlation Coefficient (r) and Adjusted R values of the variables investigated. This was further interpreted using Cohen's (1988) r and R values interpretation. The interpretation of the data analysis is based on standard provision from Pallant (2010) and Hair, Hult, Ringle and Sarstedt (2016). The objective is to provide answers to the research questions by identifying the pattern of the data analysis. Reporting of the entire research process is in line with the standard, with keen attention to the relationship with the theories used in this study. The reporting is presented in Chapter Six.

4.6 Pilot Study

A pilot study is a preliminary small investigation to assess the feasibility of a proposed study, as well as the time and cost involved and to improve the study design. It enables the researcher to test the research process, standardise procedures and to witness the research design in practice. It examines whether the study is worth the proposed time, effort and resources and pre-tests the research instrument (Sim and Wright, 2005). However, an important way to carry out an effective analysis is by depending on pilot data.

Furthermore, to achieve an error-free, precise and comprehensive questionnaire, it was piloted across the three banks in Lagos State. In Bank A, four people (the manager, operation manager and IT personnel) participated in the study. In Bank B, seven individuals participated, viz., the head of operations, area manager, IT department manager and three junior staff. Finally, in Bank C, four senior and junior staff which comprised of managers and heads of operations participated. The pilot study lasted two weeks because of the limited time available to accomplish this research. The participants agreed that the questionnaire was good for, and in line with, the study.

4.7 Ethical Clearance

Researchers need to adhere to ethical standards in order to achieve credible results. A letter was sent to each of the banks where data would be collected, stating the research objectives and that the study was being conducted solely for academic purposes. All the study respondents signed letters indicating that they understood the purpose of the study. The questions in the survey instrument were tailored for easy understanding and flexible responses that guaranteed that the respondents were not coerced into supporting particular responses. Ethical approval was sought and obtained from UKZN before the study commenced and the researcher complied with all the ethical norms and regulations set down by the University. The gate-keepers' letters and the ethical clearance are in Appendices C and E, respectively.

4.8 Chapter Summary

This chapter discussed the methods employed to achieve the study's objectives and the justification for their adoption. It presented the step-by-step phases employed, including the choice of respondents; the sample size in relation to the population; and the sampling strategy. It was noted that the study adopted a quantitative approach and used a survey questionnaire to gather data and SPSS software for data analysis. The process followed to design the items of the survey instrument was also discussed in relation to the investigated variables and their respective dimensions and measurements.

The next chapter presents, analyses and interprets the data using the reliability test, descriptive analysis and the various relationships amongst the constructs.

CHAPTER FIVE
DATA ANALYSIS AND INTERPRETATION

5.1 Introduction

This chapter presents the analysis and interpretation of the data collected on ISSsPs compliance by Nigerian banks. The findings include the response rate to the survey questionnaire, the respondents' demographic characteristics, a descriptive analysis of the constructs and the testing of hypotheses. The level of significance is also presented.

5.2 Overview of Data Analysis

Here the various methods applied to carry out the analysis in this study are explained. Since this study employed quantitative methods, the analysis is done quantitatively. The chi-square goodness of fit, chi-square test of independence and the binomial test were administered. The chi-square goodness of fit test is good in measuring how well the distribution of data fits with the expected value (Lani, 2011). Similarly, McHugh (2013) acknowledged that a chi square test is good at identifying whether a significant relationship exists between two categorical variables. On the other hand, the binomial test is best used to determine the number of 'successes' in a binary experiment.

5.2 Response Rate

A total of 370 survey questionnaires were distributed to the study population, of which 355 were completed and returned. This represents a 95.95% response rate. Table 5.1 presents the response rate.

Table 5.1: Response Rate

	Frequency	Percentage (%)
Number of Questionnaires Distributed	370	100
Number of Questionnaires Returned	355	95.95
Number of Questionnaires Not Returned	15	4.05

5.3 Missing Data

The impact of missing data varies with respect to its occurrence and magnitude. A missing data rate of 1% is not considered to pose any threat, while 5% is regarded as bearable and

manageable as long as the data is missing completely at random (MCAR), whilst 15% is said to pose a significant threat, calling for sophisticated techniques to resolve this issue (Acuna and Rodrigues, 2004). Appendix F presents the table of the missing values in this study, amounting to less than 2%. The missing value in this study is bearable and therefore treated by applying pairwise deletion across all the data sets, since the pairwise deletion is the default in SPSS 25.0. The purpose of imploring pairwise deletion is that it avoids wastefulness of data and gives a guarantee of obtaining unbiased results in statistical analysis, as compared to other methods for missing value treatments (Van Ginkel, 2020). Pairwise deletion is applied to treat missing values case by case in each construct in this study, which covers correlation, regression, factor analysis and covariance matrix generally. The application of pairwise deletion in this study removes all the columns and rows with empty value and presents only the data sets that are captured with values.

5.4 Demographic Characteristics of the Respondents

The frequency distribution of the respondents' job descriptions shows that the majority of the respondents (35.5%) are in the IT department, followed by system maintenance (7.3%), internal control (6.8%), customer care (5.1%), quality control (2.5%), bank managers (2.5%) and heads of operations (2.3%). However, the descriptive analysis revealed that 38% of the responses were missing. The descriptive analysis also revealed that 24.8% of the respondents had less than three years work experience, while 37.7% had between three and five years, 27.3% from six to nine years and 9.3% more than 10 years' experience. A further 0.8% of the responses were missing. A large proportion of the respondents (38%) have bachelor's degrees; 26% hold a diploma; whilst 23.1% have masters' degrees; 3.1% PhDs and 0.3% other degrees. However, 9% of the responses were missing. The respondents' demographic characteristics are presented in Table 5.2 and Figures 5.1 to 5.3.

Table 5.2: Demographic Characteristics of the Respondents

Construct	Items	Frequency	Percentage (%)
Job Description	IT	126	35.5
	Customer care	18	5.1
	Head of operations	8	2.3
	Quality control	9	2.5
	Internal control	24	6.8
	System maintenance	26	7.3
	Bank managers	9	2.5
	Unspecified	135	38.0
Experience	<3 years	88	24.8
	3 - <6 years	134	37.7
	6 - <10 years	97	27.3
	10+ years	33	9.3
	Unspecified	3	.8
Education	Diploma	94	26.5
	Bachelor's degree	135	38.0
	Master's degree	82	23.1
	Doctoral degree	11	3.1
	Other	1	.3
	Unspecified	32	9.0

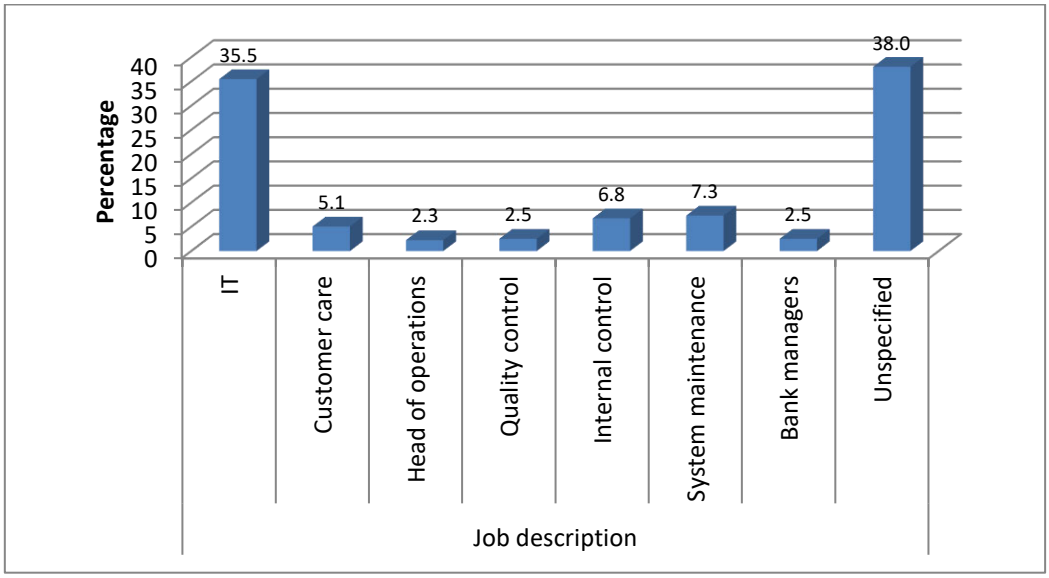


Figure 5.1: Distribution of the Respondents' Job Descriptions

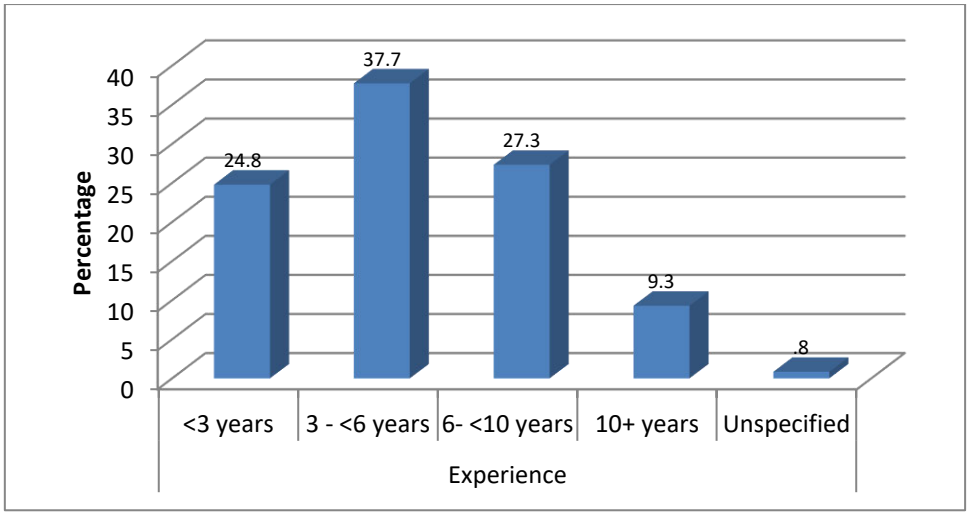


Figure 5.2: Distribution of the Respondents' Experience

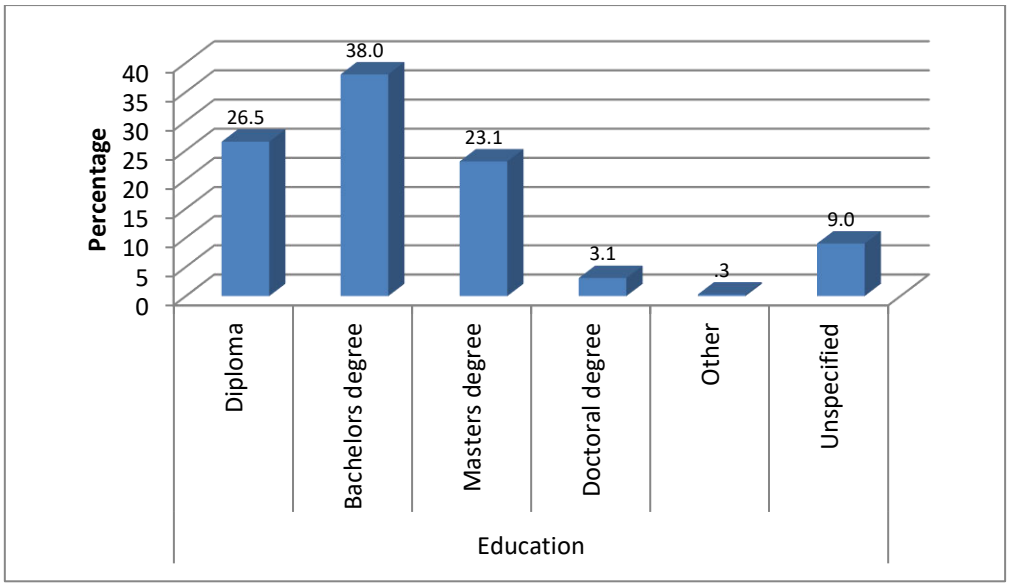


Figure 5.3: Distribution of the Respondents' Educational Qualifications

5.5 Descriptive Analysis of ISSsPs Compliance Rate amongst Nigerian Banks

The frequency distribution of the rate of ISSsPs review by Nigerian banks revealed that the majority of the respondents' (51.3%) banks review their ISSsPs at least once a year; followed by 16.6% that do so at least once every six months; 11.3% that review their ISSsPs at least once a month; and 10.7% which review their ISSsPs at least once every quarter. A Chi-square test was conducted for the goodness of fit to indicate if any of the responses was selected significantly more than the others and the findings revealed a significant number (182, 51.3%),

which indicates that their organisations review their ISSs policies at least once a year, p<.0005. The description of the rate of review of ISSsPs policy is presented in Table 5.3 and Figure 5.4.

Table 5.3: ISSsPs Compliance Rate

Items	Frequency	Percentage (%)
Less than once a year	29	8.2
At least once a year	182	51.3
At least once every 6 months	59	16.6
At least once every quarter	38	10.7
At least once a month	40	11.3
Non-response	7	2.0
Total	355	100

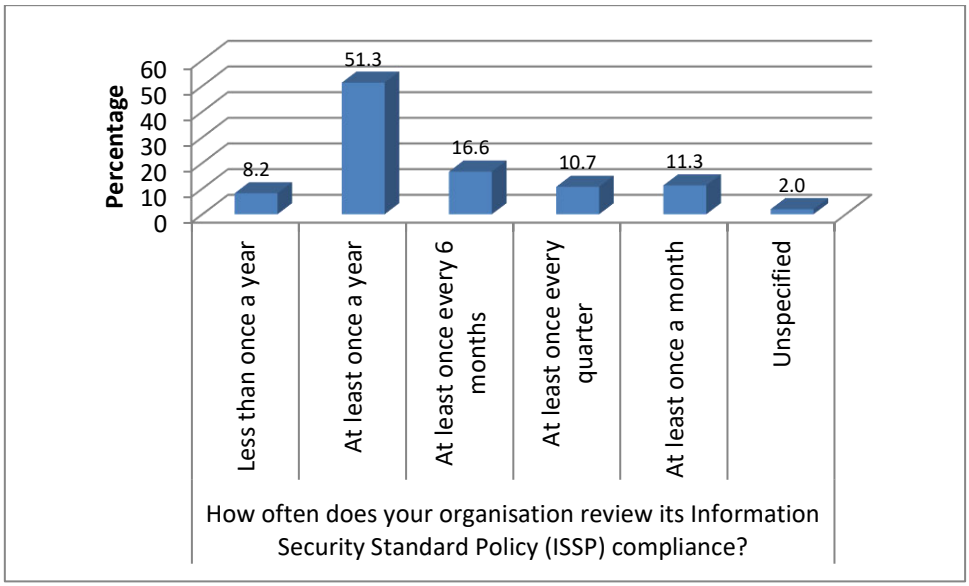


Figure 5.4: Rate of Review of ISSsPs in Nigerian Banks

A further descriptive analysis was conducted on the type of ISSsPs subscribed to by the banks. As shown in Table 8.4, 86.5% of the banks subscribed to FISMA, 86.8% to HIPAA, 63.9% subscribed to SOX and 93.3% subscribed to ISO/IEC 17799. Only 6.2% of the banks subscribed ISO/IEC 27001 and ISO/IEC 27002.

A binomial test was conducted to establish if one option was preferred over the other. The result shows that none of the options was selected by a significant proportion of the respondents.

Table 5.4: ISSsPs Subscription by Nigerian Banks

ISSPs	Items	Frequency	Percent (%)
FISMA	Yes	48	13.5
	No	307	86.5
HIPAA	Yes	42	11.8
	No	308	86.8
	Missing Data	5	1.4
SOX	Yes	128	36.1
	No	227	63.9
ISO/IEC 17799	Yes	181	51.0
	No	172	48.5
	Missing Data	2	.6
GLBA	Yes	22	6.2
	No	332	93.5
	Missing Data	1	.3
OTHER	Yes	22	6.2
	No	332	93.5
	Missing Data	1	.3

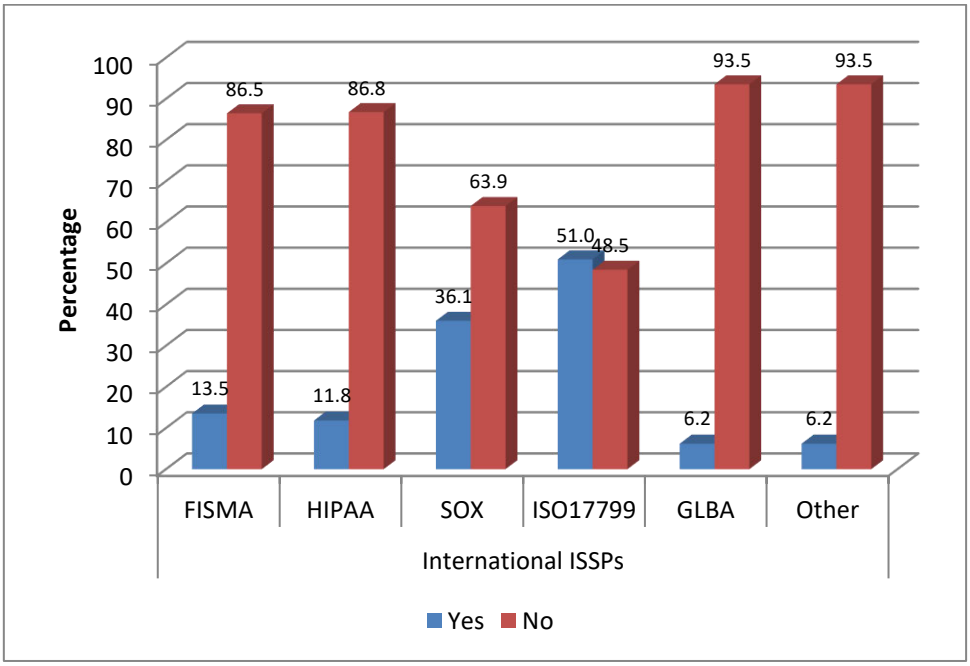


Figure 5.5: ISSsPs Subscription by Nigerian Banks

The descriptive analysis also revealed that 34.4% of the respondents indicated that a new ISS policy had been adopted in the past 6-12 months, while 29.3% responded that a new policy had been adopted over a year ago; 17.7% stated that this had occurred in the past three months and 14.4% indicated that a new ISSsPs had been adopted in the past three to six months. However, 4.2% of the responses were missing. A Chi-square test revealed that a significant number of the respondents (182, 51.3%) believed that their organisations review their ISSsPs at least once a year, $p<0.05$. The description of the rate of review of ISSsPs is presented in Table 5.5 and

Figure 5.6. A binomial test was conducted to determine if there ws a preferred option. The result shows that a new ISSsPs is adopted every 6-12 months.

Table 5.5: Adoption of New ISSsPs Policies

Items	Frequency	Percentage (%)
>1 year ago	104	29.3
6-12 months ago	122	34.4
3-6 months ago	51	14.4
In the past 3 months	63	17.7
Non-response	15	4.2

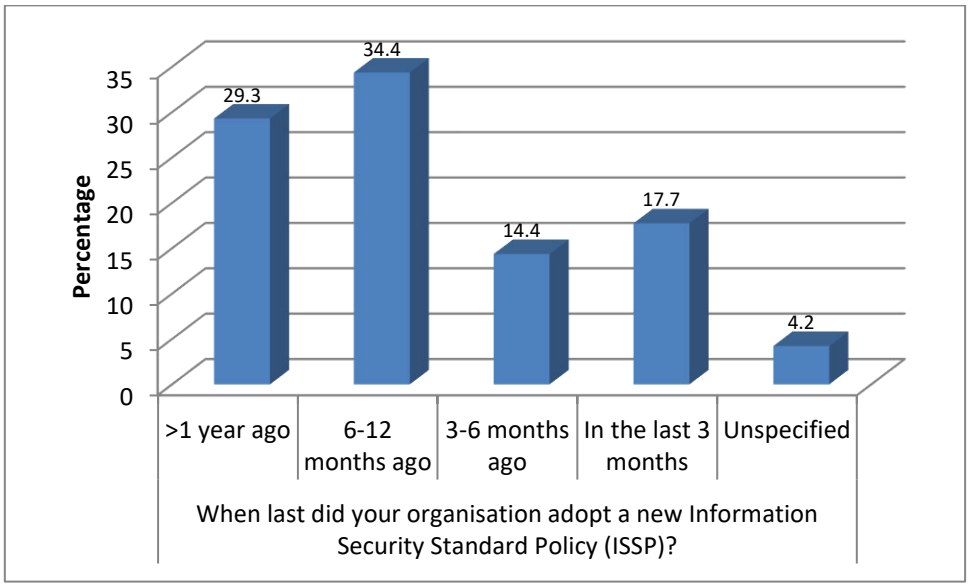


Figure 5.6: Adoption of a New Information System Policy

5.6 Experiences of Information Security Breaches

The results of the descriptive analysis of information security breach experiences in Table 5.7 show that 45.4% of the banks in the sample experienced information security breaches at least once a year, followed by 18.9% at less than once a year, 13.5% at once every 6 months and once every quarter, respectively; while 8.7% experienced information security breaches at least once a month. A further bivariate test indicated that the majority of the banks experienced information security breaches at least once a year.

Table 5.6: Descriptive Analysis of Information Security Breach Experiences

Items	Frequency	Percentage (%)
Less than once a year	67	18.9
At least once a year	161	45.4
At least once every 6 months	48	13.5
At least once every quarter	48	13.5
At least once a month	31	8.7

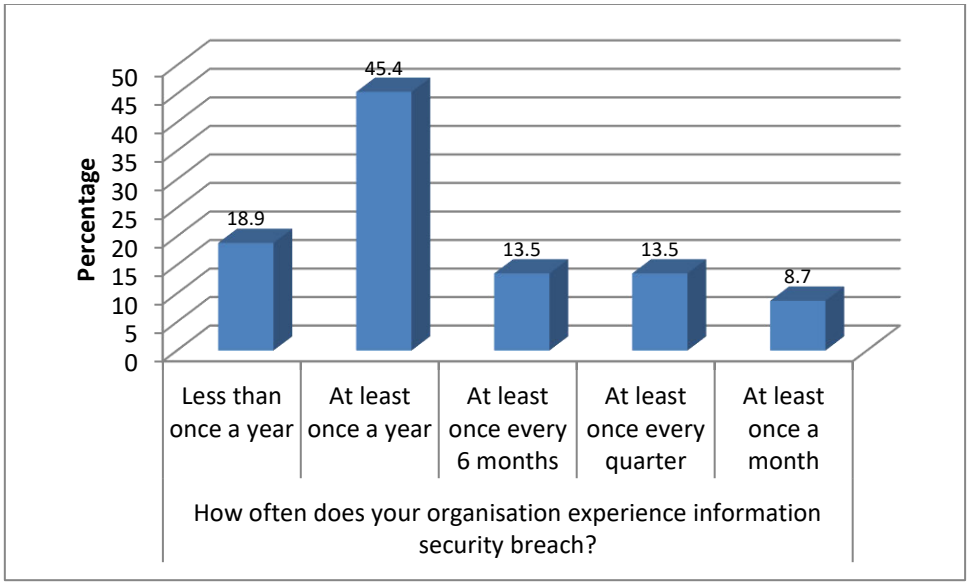


Figure 5.7: Information security breach experiences

Descriptive analysis on international ISSsPs which successfully prevent information security breaches shows that 93.8% of the respondents indicated that FISMA does not successfully prevent information security breaches, while 89.3% identified HIPAA, 78% SOX and 93.2% GLBA as not being successful in preventing information security breaches. Only ISO/IEC 17799 was regarded as being successful in preventing information security breaches in Nigerian banks. A further binomial test indicated that "No" is the significant response on the international ISSsPs that successfully prevent information security breaches. Table 5.7 presents the responses on international ISSsPs that successfully prevent information security breaches amongst Nigerian banks.

Table 5.7: Prevention of Information Security Breaches by ISSsPs

ISSPs	Items	Frequency	Percentage (%)
FISMA	Yes	22	6.2
	No	333	93.8
	Total	355	100.0
HIPAA	Yes	37	10.4
	No	317	89.3
	Total	354	99.7
	Missing Data	1	.3
SOX	Yes	77	21.7
	No	278	78.3
	Total	355	100.0
ISO/IEC 17799	Yes	218	61.4
	No	130	36.6
	Total	348	98.0
	Missing Data	7	2.0
GLBA	Yes	23	6.5
	No	331	93.2
	Total	354	99.7
	Missing Data	1	.3
OTHER	Yes	6	1.7
	No	349	98.3
	Total	355	100.0

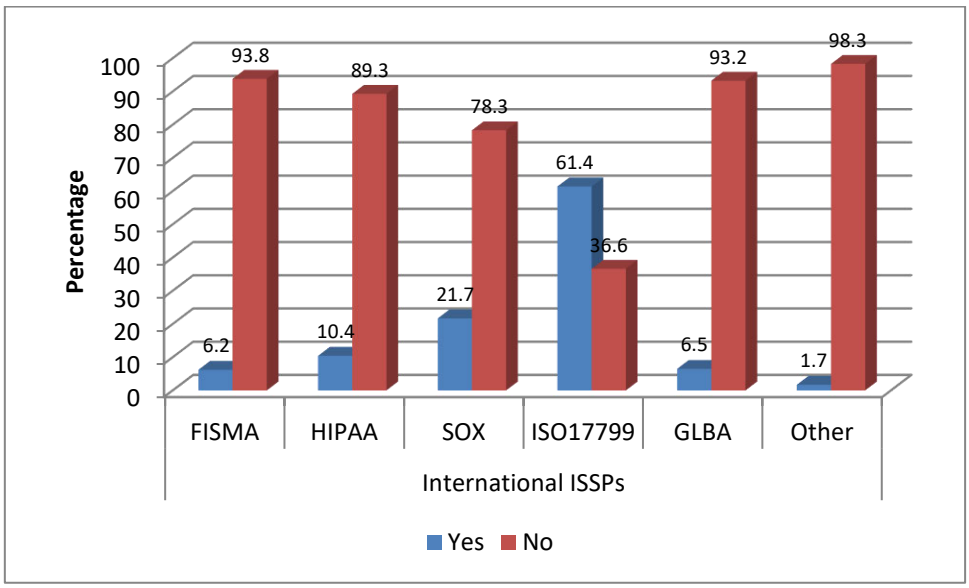


Figure 5. 8: Prevention of Information Security Breaches by ISSsPs

The descriptive analysis conducted to determine the last time the organisations successfully averted a pending information security breach revealed that 33.8% did so more than a year ago; 18% never averted a pending information security breach; 16% of the banks averted an information security breach between six months and a year ago; and 13.2% between three and six months ago and in the past three months, respectively. A further bivariate test showed that

a pending information security breach was averted over a year ago. Table 5.8 and Figure 5.9 present the results.

Table 5.8: Aversion of Pending Information Security Breach

Description	Frequency	Percentage
Never	64	18.0
More than a year ago	120	33.8
Between 6 months and a year ago	59	16.6
Between 3 and 6 months ago	47	13.2
In the last 3 months	47	13.2
Non- response s	18	5.1

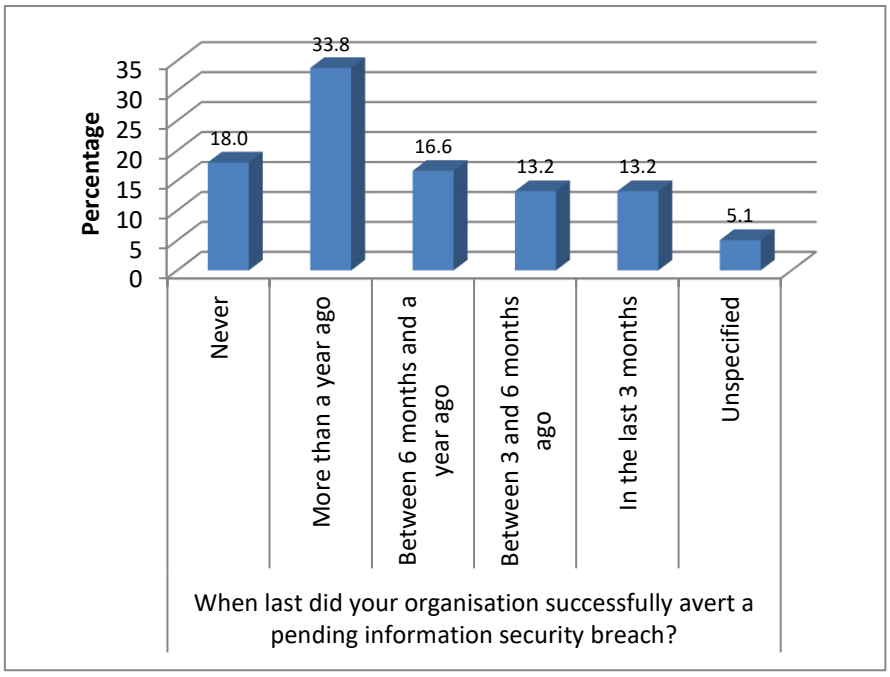


Figure 5.9: Aversion of Pending Information Security Breaches by Bank

5.7 Descriptive Analysis of Constructs

This section presents the description of the constructs of the study. The mean score and one-sample test are presented to describe the respondents' agreement/disagreement with the constructs.

5.7.1 Perceived Information Security Compliance

Table 5.9 and Figure 9.10 present the findings of the descriptive analysis conducted on perceived information security compliance. It revealed a mean score = 5.28 for "my organisation's information security policy is consistently updated on a periodic basis". The

results further show a mean score of 5.40 for "my organisation's information security policy evolves as technology changes", while "My organisation complies with major ISSsPs" and "ISSsPs compliance is part of the organisation's core values" have a mean score of 5.44. Finally, the mean score of 5.53 indicates significant agreement with "There is a review system for our information security policy standard in my organisation".

Table 5.9: Description of Perceived Information Security Compliance

Code	Description	Mean	Std. Deviation	Std. Error Mean
ISS01	My organisation's information security policy is consistently updated on a periodic basis.	5.28	2.127	.113
ISS02	My organisation's information security policy evolves as technology changes.	5.40	1.947	.104
ISS03	There is a review system for our information security policy standard in my organisation.	5.53	1.788	.095
ISS04	My organisation complies with major ISS policies.	5.44	1.791	.095
ISS05	ISS policy compliance is part of the organisation's core values.	5.44	1.754	.093

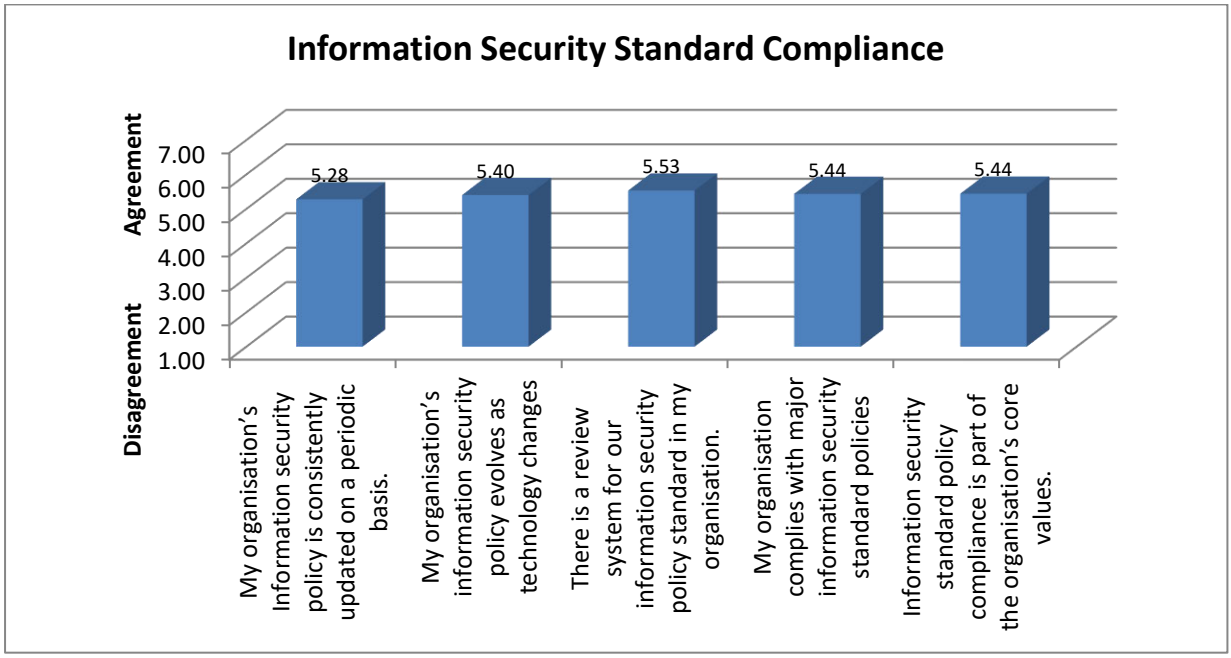


Figure 5.10: Perceived Information Security Compliance

Further analysis, known as the one sample test, was conducted to show the significance of the respondents' agreement/disagreement with the items pertaining to perceived information security compliance. The results in Table 5.9 and Figure 5.10 indicate that there is agreement

that information security policies are consistently updated on a periodic basis (M=5.28 SD=2.127), t(352) = 11.284, p<.0005; IS policies evolve as technology changes (M=5.40, SD=1.947), t (350) = 13.517, p<.0005; there is a review system for our information security policy standards in my organisation (M = 5.53, SD = 1.788), t(352) = 16.100, p< 0.005; my organisation complies with major ISS policies (M = 5.44, SD = 1.791), t(352) = 15.069, p<0.005; and ISS policy compliance is part of the organisation's core values (M = 5.44, SD = 1.754), t(352) = 15.445, p < 0.005.

5.7.2 Normative Belief

The results of the descriptive analysis of the normative belief construct presented in Table 5.10 indicate that there is agreement amongst the respondents that "it is important to me for my co-workers to see me as an ethical person" (M = 5.22, SD = 1.961), t(351) = 11.679, p < 0.005; "My co-workers believe I should comply with information security policy standards" (M = 5.50, SD = 1.770), t(352) = 15.941, p < 0.005; "I comply with ISS because my superior assesses my work" (M = 5.32, SD = 1.822), t(349) = 13.583, p < 0.005; "My co-workers believe it is important to comply with information security policy standards" (M = 5.59, SD = 1.633), t(349) = 18.218, p < 0.005; and "To my knowledge, the majority of employees comply with the organisation's IS security policies" (M = 5.54, SD = 1.608), t(353) = 17.977, P < 0.005.

Table 5.10: Normative belief

Code	Description	Mean	Std. Deviation	Std. Error Mean
NOB01	It is important to me for my co-workers to see me as an ethical person.	5.22	1.961	.105
NOB02	My co-workers believe I should comply with information security policy standards.	5.50	1.770	.094
NOB03	I comply with inform security standards because my superior assesses my work.	5.32	1.822	.097
NOB04	My co-workers believe it is important to comply with information security policy standards.	5.59	1.633	.087
NOB05	To my knowledge, the majority of employees comply with the organisation's IS security policies.	5.54	1.608	.086

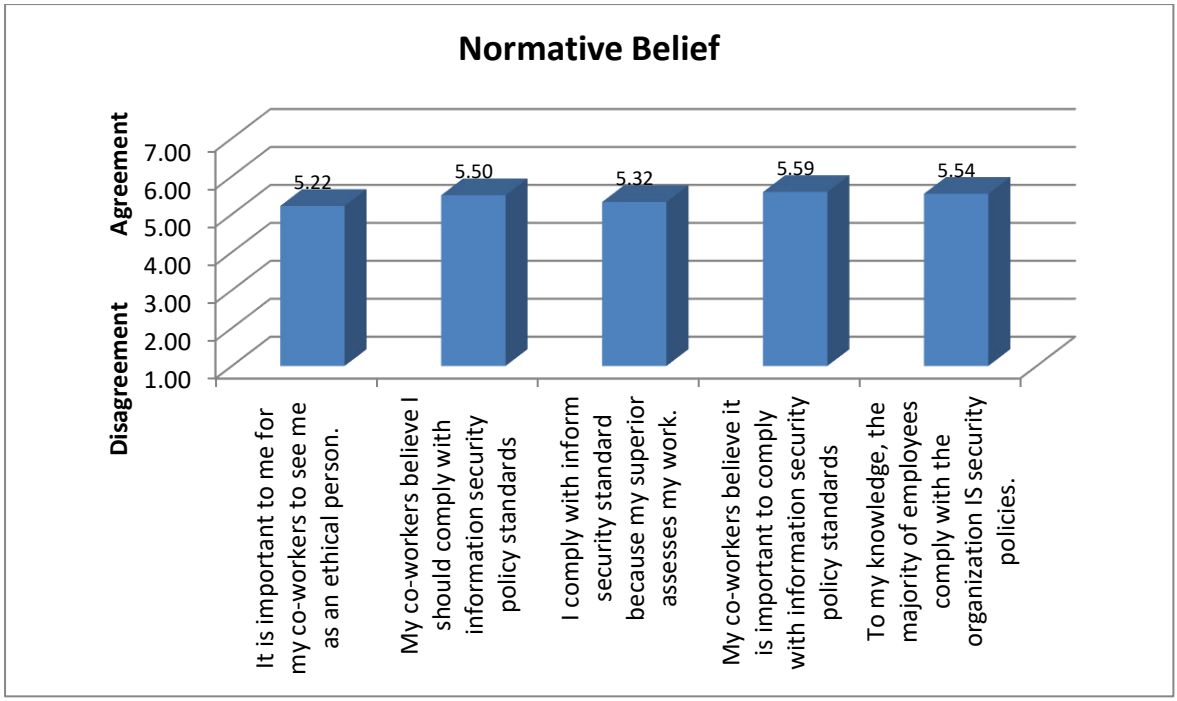


Figure 5.11: Normative Belief

5.7.3 Information Security Threats Awareness

The descriptive analysis of information security threat awareness shown in Table 5.11 reveals that there is a significant agreement amongst the respondents that they clearly understand the implications of violating security policies ($M = 5.49$, $SD = 1.968$), $t(350) = 14.157$, $P < 0.005$; they have received training on information security ($M = 5.50$, $SD = 1.758$), $t(350) = 15.970$, $P < 0.005$; security threat information has been communicated to them ($M = 5.61$, $SD = 1.569$), $t(349) = 19.251$, $P < 0.005$; they know about a continuous awareness programme on general information security threats ($M = 5.49$, $SD = 1.694$), $t(343) = 16.330$, $P < 0.005$; information security training was included as part of their orientation ($M = 5.52$, $SD = 1.632$), $t(349) = 17.459$, $P < 0.005$; information security policies are discussed during their annual evaluation ($M = 5.59$, $SD = 1.561$), $t(349) = 19.035$, $P < 0.005$; and that their supervisor updates them on changes to information security procedures ($M = 5.65$, $SD = 1.545$), $t(348) = 19.987$, $P < 0.005$.

Table 5.11: Information Security Threat Awareness

Code	Description	Mean	Std. Deviation	Std. Error Mean
STA01	I clearly understand the implications of violating security policies.	5.49	1.968	.105
STA02	I have received education about information security threats.	5.50	1.758	.094
STA03	Information regarding security threats has been communicated to me.	5.61	1.569	.084
STA04	I know about a continuous awareness programme on general information security threats.	5.49	1.694	.091
STA05	Information security training was included as part of my orientation.	5.52	1.632	.087
STA06	Information security policies are discussed during my annual evaluation.	5.59	1.561	.083
STA07	My supervisor updates me on changes to information security procedures.	5.65	1.545	.083

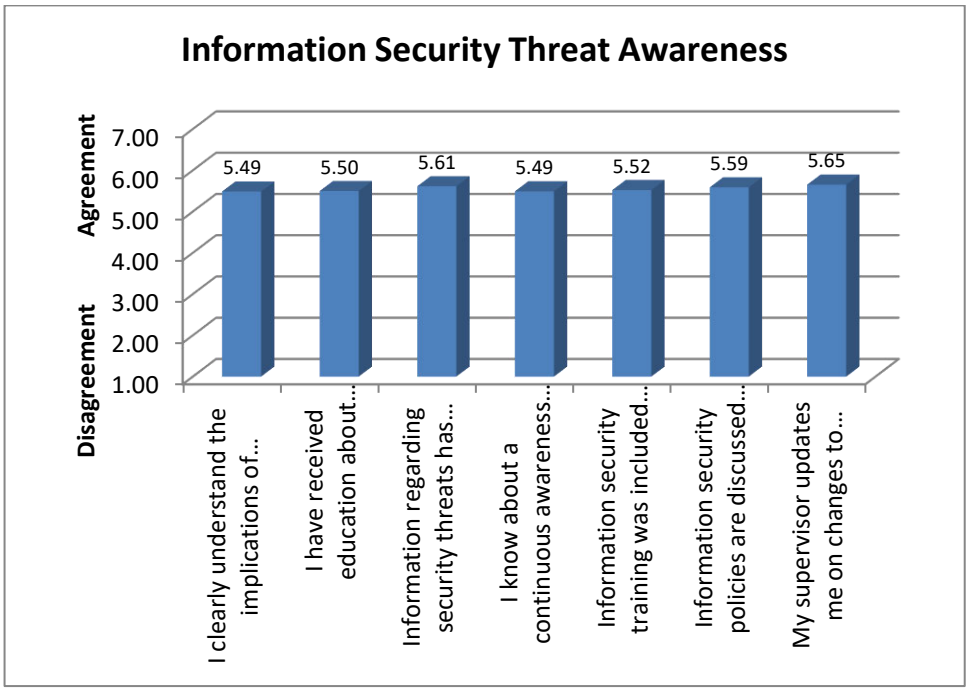


Figure 5.12: Information Security Threat Awareness

5.7.4 Perceived Effectiveness of ISSsPs Compliance

As shown in Table 5.12, the findings of the descriptive analysis of the perceived effectiveness of IS policy compliance indicate significant agreement amongst the respondents that "information security policy is effective in achieving our organisational goals for information security" ($M = 5.59$, $SD = 1.852$), $t(347) = 16.008$, $P < 0.005$; "information security policy helps to accomplish the information security objectives" ($M = 5.66$, $SD = 1.549$), $t(349) = 20.021$, $P < 0.005$; "information security policy keeps the risk at a minimum" ($M = 5.69$, $SD = 1.671$), $t(345) = 17.657$, $P < 0.005$; "compliance with the requirements of the information security policy reduces security risks" ($M = 5.68$, $SD = 1.460$), $t(345) = 21.352$, $P < 0.005$; "compliance with the requirements of the ISP secures our infrastructure" ($M = 5.68$, $SD = 1.381$), $t(349) = 22.794$, $P < 0.005$; and "overall, information security policy is effective in securing information at this organisation" ($M = 5.78$, $SD = 1.472$), $t(349) = 22.580$, $P < 0.005$.

Table 5.12: Perceived Effectiveness of ISSsPs Compliance

Code	Description	Mean	Std. Deviation	Std. Error Mean
PEF01	Our information security policy is effective in achieving our organisational goals for information security.	5.59	1.852	.099
PEF02	Our information security policy helps to accomplish the information security objectives.	5.66	1.549	.083
PEF03	Our information security policy keeps the risk at a minimum.	5.59	1.671	.090
PEF04	Compliance with the requirements of the information security policy reduces security risks.	5.68	1.460	.079
PEF05	Compliance with the requirements of the ISP secures our infrastructure.	5.68	1.381	.074
PEF06	Overall, the information security policy is effective in securing information at this organisation.	5.78	1.472	.079

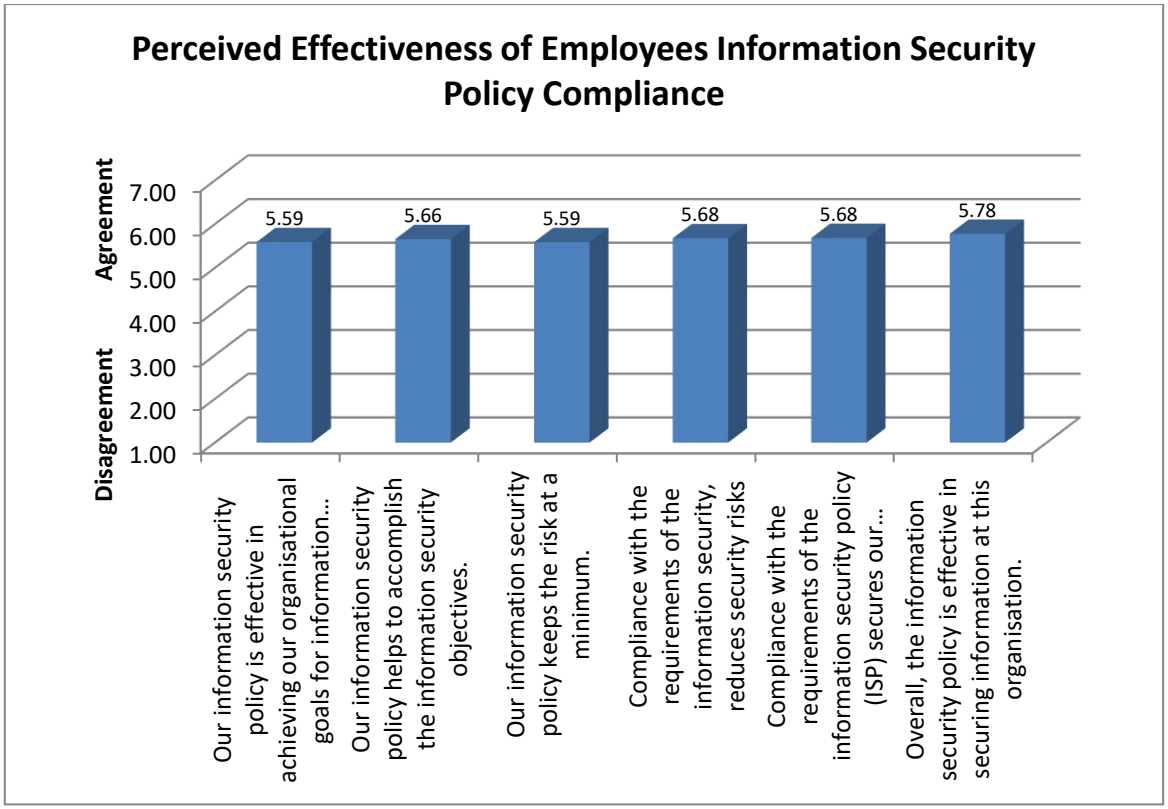


Figure 5.13: Perceived Effectiveness of Employees ISSs Policies Compliance

5.7.5 Perception Bias

Table 5.13 presents the descriptive analysis of the perception bias construct. The findings reveal that there is significant agreement amongst the respondents that "In case of an information security threat, I always act swiftly no matter the severity of the threat" ($M = 5.43$, $SD = 1.978$), $t(349) = 13.484$, $P < 0.005$; "The measures in place to counteract information security threats are suitable and work successfully" ($M = 5.47$, $SD = 1.861$), $t(349) = 14.760$, $P < 0.005$; "The measures we use to counteract information security threats can successfully deal with the most complex of threats" ($M = 5.41$, $SD = 1.669$), $t(349) = 15.742$, $P < 0.005$; "The security-resisting mechanisms in place are successful in counteracting most threats that we experience" ($M = 5.37$, $SD = 1.740$), $t(348) = 14.707$, $P < 0.005$; "If I am unsure about a possible security threat, I prefer to take swift preventative measures rather than ignore it and have to fix it after it has happened" ($M = 5.61$, $SD = 1.657$), $t(350) = 18.195$, $P < 0.005$; "The organisation sets high standards for the protection of its information assets" ($M = 5.66$, $SD = 1.640$), $t(348) = 18.966$, $P < 0.005$; "Overall, compliance with the Information Security Policy at this organisation is good" ($M = 5.64$, $SD = 1.610$), $t(349) = 19.057$, $P < 0.05$; and "The

policies in place regarding information security are adequate to address security threats" (M = 5.61, SD = 1.681), t(348) = 17.865, P < 0.005.

Table 5.13: Perception Bias

Code	Description	Mean	Std. Dev	Std. Error Mean
PCB01	In case of an information security threat, I always act swiftly no matter the severity of the threat.	5.43	1.978	.106
PCB02	The measures in place to counteract information security threats are suitable and work successfully.	5.47	1.861	.099
PCB03	The measures we use to counteract information security threats can successfully deal with the most complex of threats.	5.41	1.669	.089
PCB04	The security-resisting mechanisms in place are successful in counteracting most threats that we experience.	5.37	1.740	.093
PCB05	If I am unsure about a possible security threat, I prefer to take swift preventative measures rather than ignore it and have to fix it after it has happened.	5.61	1.657	.088
PCB06	The organisation sets high standards for the protection of its information assets.	5.66	1.640	.088
PCB07	Overall, compliance with the Information Security Policy at this organisation is good.	5.64	1.610	.086
PCB08	The policies in place regarding information security are adequate to address security threats	5.61	1.681	.090

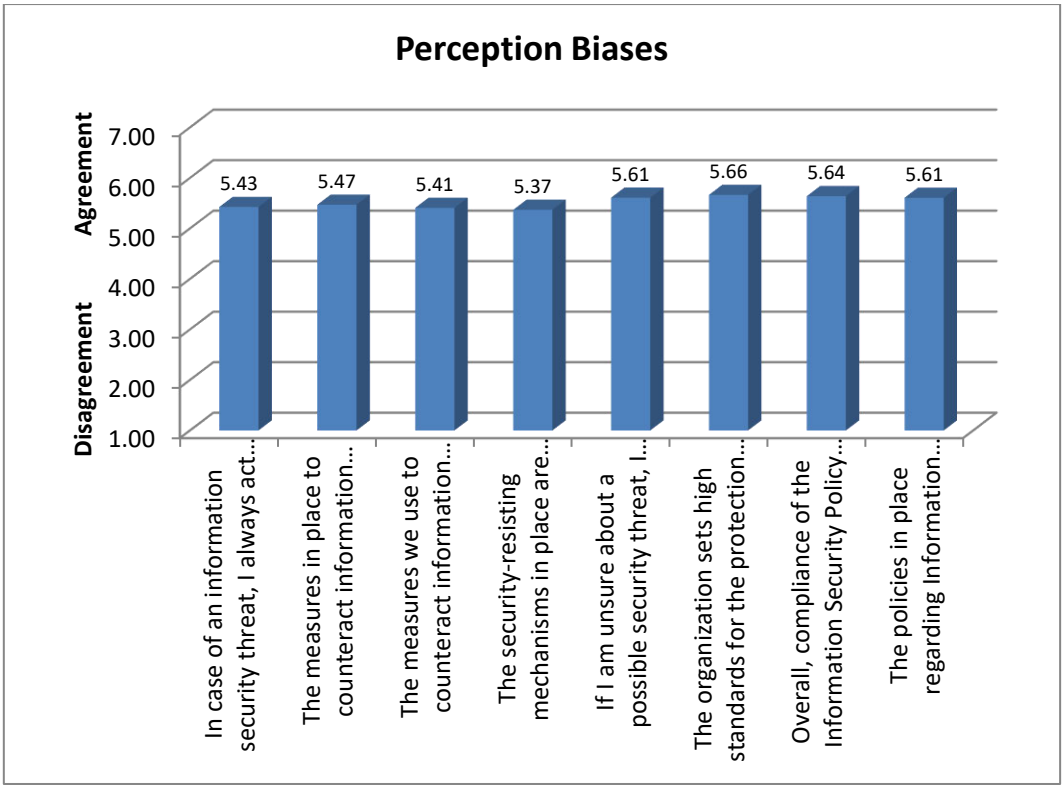


Figure 5.14: Perception Bias

5.7.6 Certainty of Detection

The results of the descriptive analysis shown in Table 6.14 reveal significant agreement amongst the respondents that "My computer practices are properly monitored for policy violations" ($M = 5.36$, $SD = 1.964$), $t(349) = 12.927$, $P < 0.005$; "If I violate organisational security policies, I will most likely be caught" ($M = 5.55$, $SD = 1.761$), $t(350) = 16.462$, $P < 0.005$; "My computer is monitored for security threat exposure at random times of which I am unaware" ($M = 5.47$, $SD = 1.720$), $t(350) = 16.043$, $P < 0.005$; "I am assessed for information security compliance" ($M = 5.65$, $SD = 1.586$), $t(349) = 19.447$, $P < 0.005$; and "My computer is routinely checked for security threats at regular intervals" ($M = 5.58$, $SD = 1.619$), $t(350) = 18.263$, $P < 0.005$.

Table 5.14: Certainty of Detection

Code	Description	Mean	Std. Deviation	Std. Error Mean
COD01	My computer practices are properly monitored for policy violations.	5.36	1.964	.105
COD02	If I violate organisational security policies, I will most likely be caught.	5.55	1.761	.094
COD03	My computer is monitored for security threat exposure at random times of which I am unaware.	5.47	1.720	.092
COD04	I am assessed for information security compliance.	5.65	1.586	.085
COD05	My computer is routinely checked for security threat exposure at regular intervals.	5.58	1.619	.086

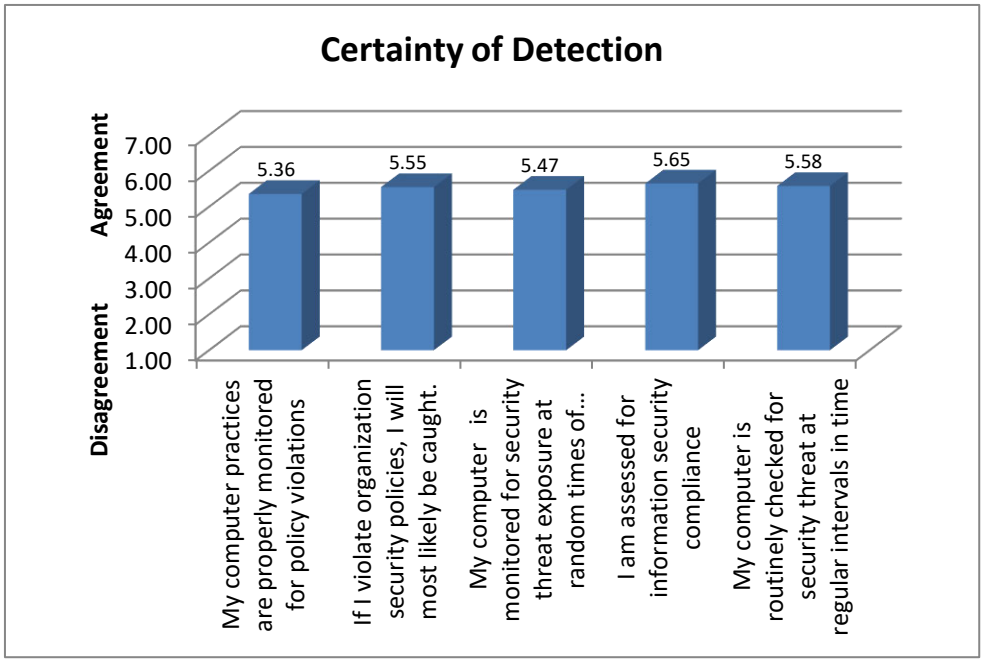


Figure 5.15: Certainty of Detection

5.7.7 Severity of Penalty

The findings on severity of penalty presented in Table 5.15 indicate that there is significant agreement amongst the respondents that "Employees caught violating security policies are appropriately corrected" ($M = 5.46$, $SD = 1.963$), $t(350) = 13.973$, $P < 0.005$; "Information security policies are enforced by punishing employees that break them" ($M = 5.66$, $SD = 1.709$), $t(348) = 18.169$, $P < 0.005$; "Serial information security offenders among employees are appropriately disciplined" ($M = 5.76$, $SD = 1.572$), $t(350) = 21.012$, $P < 0.005$; "Employees

who repeatedly break security rules can lose their jobs" (M = 5.75, SD = 1.593), t(347) = 20.525, P < 0.005; "If I were caught violating organisational information security policies, I would be severely punished" (M = 5.64, SD = 1.557), t(350) = 19.743, P < 0.005; and "My employer takes strict action against violation of information security policy" (M = 5.89, SD = 1.521), t(350) = 23.299, P < 0.005.

Table 5.15: Severity of Penalty

Code	Description	Mean	Std. Deviation	Std. Error Mean
SOP01	Employees caught violating security policies are appropriately corrected.	5.46	1.963	.105
SOP02	Information security policies are enforced by punishing employees that break them.	5.66	1.709	.091
SOP03	Serial information security offenders among employees are appropriately disciplined.	5.76	1.572	.084
SOP04	Employees who repeatedly break security rules can lose their jobs.	5.75	1.593	.085
SOP05	If I were caught violating organisational information security policies, I would be severely punished.	5.64	1.557	.083
SOP06	My employer takes strict action against violation of information security policy.	5.89	1.521	.081

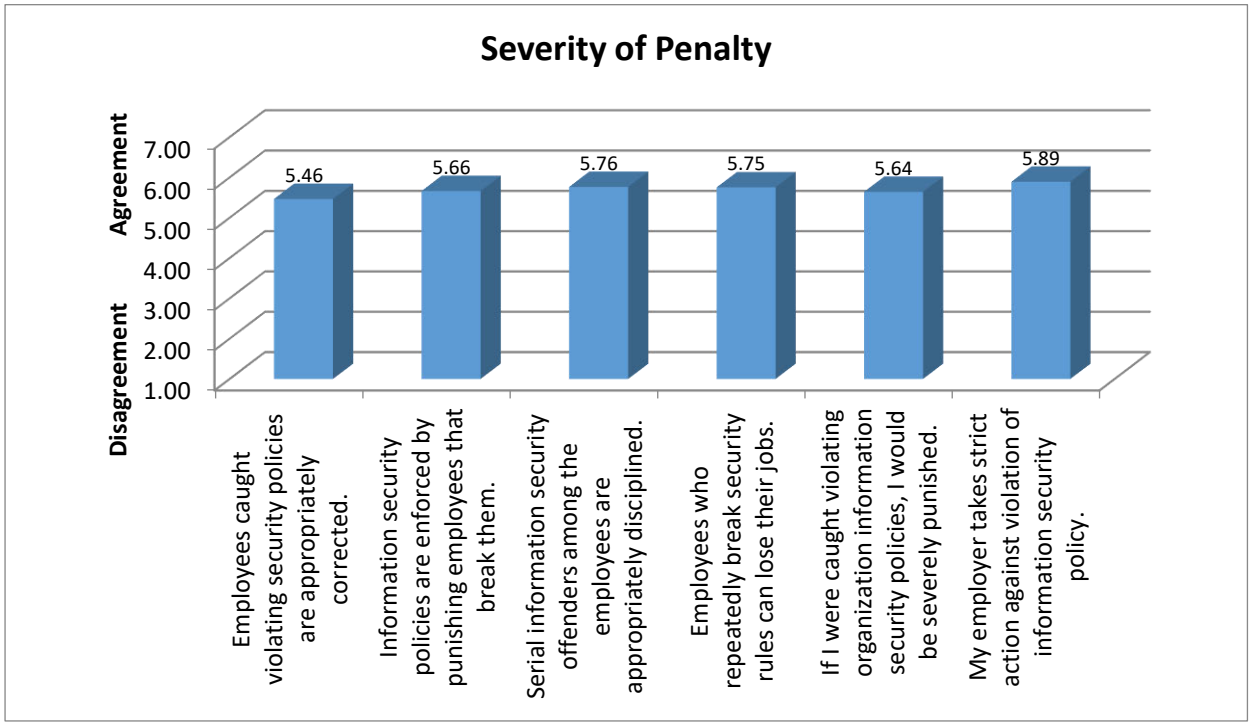


Figure 5.16: Severity of Penalty

5.7.8 Employee Behavioural Intention to Comply

The findings of the descriptive analysis of employee behavioural intention to comply shown in Table 5.16 indicate significant agreement with protecting information and technology resources according to the requirements of the ISSsPs of my organisation (M = 5.56, SD = 1.782), t(349) = 16.378, P < 0.005; carrying out responsibilities as prescribed in the ISSsPs in order to ensure the security of the information (M = 5.73, SD = 1.685), t(349) = 19.189, P < 0.005; complying with information security procedures (M = 5.79, SD = 1.539), t(349) = 21.746, P < 0.005; ignoring information security procedures that I think are not necessary (M = 5.10, SD = 2.076), t(349) = 9.915, P < 0.005; intention to follow organisational security policies wherever possible (M = 5.84, SD = 1.537 t(349) = 22.433, P < 0.005; and intention to comply with information security policies (M = 6.00, SD = 1.552), t(349) = 24.138, P < 0.005.

Table 5.16: Employees' Behavioural Intention to Comply

Code	Description	Mean	Std. Deviation	Std. Error Mean
EBI01	In my daily work, I try to protect information and technology resources according to the requirements of the ISP of my organisation.	5.56	1.782	.095
EBI02	When I use information technology, I try to carry out my responsibilities as prescribed in the ISP in order to ensure the security of the information I am working with.	5.73	1.685	.090
EBI03	When performing my daily work, I try to comply with information security procedures.	5.79	1.539	.082
EBI04	I tend to ignore information security procedures that I think are not necessary.	5.10	2.076	.111
EBI05	My intention is to follow my organisational security policies wherever possible.	5.84	1.537	.082
EBI06	I intend to comply with information security policies.	6.00	1.552	.083

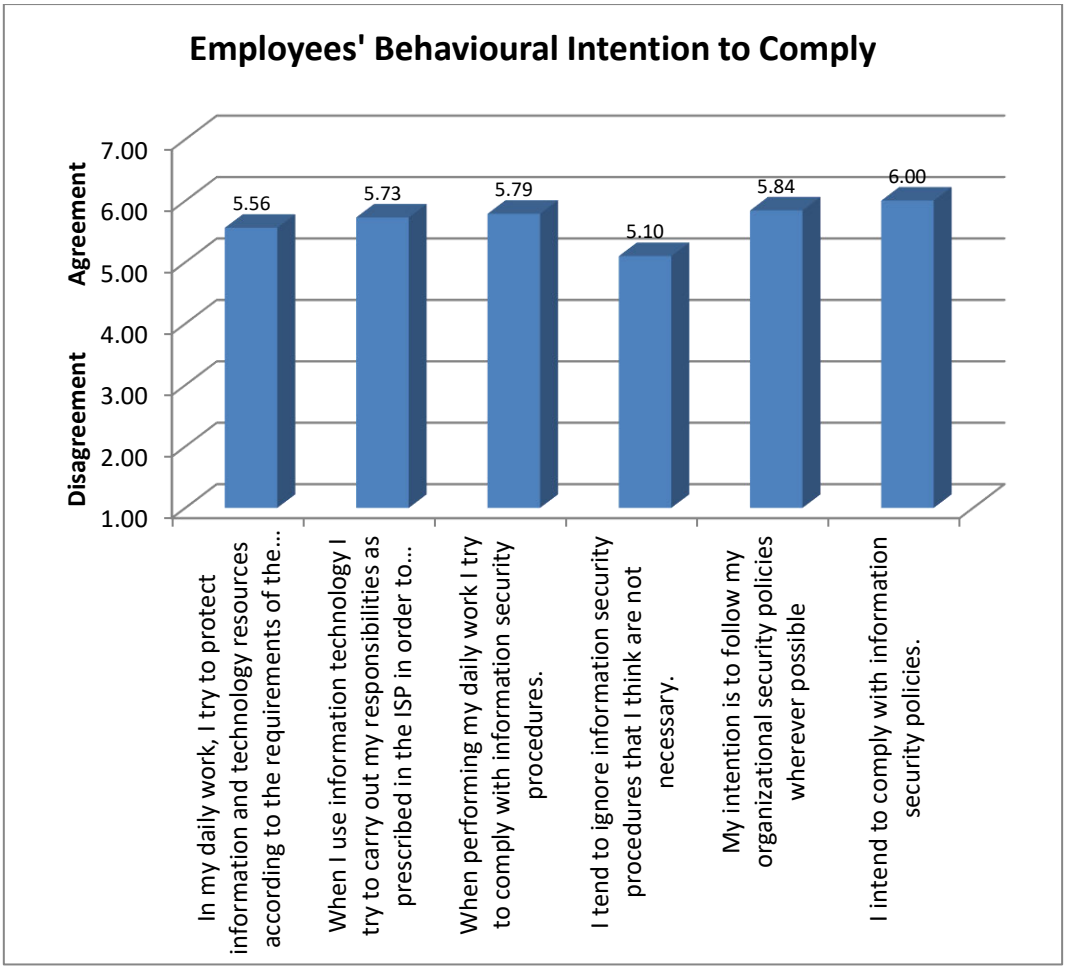


Figure 5.17: Employees' Behavioural Intention to Comply

5.8 Fundamental Assumptions of Regression

Prior to conducting the regression analysis, the assumptions of normative, linearity common method bias and homoscedasticity were checked for any violations. The following section presents the results of the assumptions of the regression analysis.

5.8.1 Common Method Bias

Common method bias is the variance that is attributable to the measurement procedure rather than the actual concept of interest to the researcher (Podsakoff, Mackenzie, Lee and Podsakoff, 2003). Many studies have investigated how to reduce or eliminate method biases,as they are one of the sources of measurement errors which may affect the validity of conclusions on the relationships between constructs (Podsakoff *et al*., 2003; Meade *et al*., 2008). Self-reported data from the Nigerian banking industry was used in this study, thereby creating the potential for the existence of common method variance. The measure of the constructs was obtained

from a single source, which could have created the possibility of the existence of common method bias (Meade *et al*., 2008). Hence, Harman's single test was conducted to address the issue of common method variance.

In this technique, all the variables are simultaneously loaded onto the exploratory factor analysis and the un-rotated factor solution is examined to detect the factors that are necessary to provide an explanation for the variables (Aulakh and Gencturk, 2000; Podsakoff *et al*., 2003). It is assumed that if a single factor emerges from the factor analysis or the covariance amongst the measures is explained by one general factor, a substantial amount of common method variance can be inferred (Podsakoff *et al*., 2003). The un-rotated exploratory factor analysis in this study indicates 19 components extracted. This implies that there is no general factor in the un-rotated factor structure. Hence, common method bias is not a serious problem in this study.

5.8.2 Test of Normality

The assumption of normality was assessed using the Kolmogorov and Smirnov test and Shapiro Wilks test. This test compares the data to normal distributions with the same mean and standard deviation (Ghasemi and Zahediasi, 2012).

Table 5.17: Test of Normality result

Constructs	**Min**	**Max**	**Mean**	**Std. Deviation**	**Skewness**		**Kurtosis**	
	Statistic	Statistic	Statistic	Statistic	Statistic	Std. Error	Statistic	Std. Error
ISS	1.00	7.00	5.4176	1.59829	-1.154	.130	.209	.259
NOB	1.00	7.00	5.4336	1.45424	-1.179	.130	.512	.259
STA	1.00	7.00	5.5480	1.37296	-1.169	.130	.495	.260
PEF	1.00	7.00	5.6593	1.26658	-1.387	.130	1.374	.260
PCB	1.29	7.00	5.5201	1.39551	-1.219	.130	.511	.260
COD	1.00	7.00	5.5194	1.45007	-1.224	.130	.620	.260
SOP	1.33	7.00	5.6942	1.38600	-1.448	.130	1.089	.260
EBI	1.00	7.00	5.7846	1.33796	-1.721	.130	2.387	.260
Valid N (listwise)								

Two measures were used to confirm the distribution of data: skewness and kurtosis. Skewness measures the extent to which a variable's distribution is symmetrical, whilst kurtosis determines whether the distribution is too peaked or shallow. The result of the normality test shown in Table 5.18 indicates that statistics and standard error for both the skewness and kurtosis are insignificant (P > 0.05), implying that all the variables for this study fall within the accepted margin for normality.

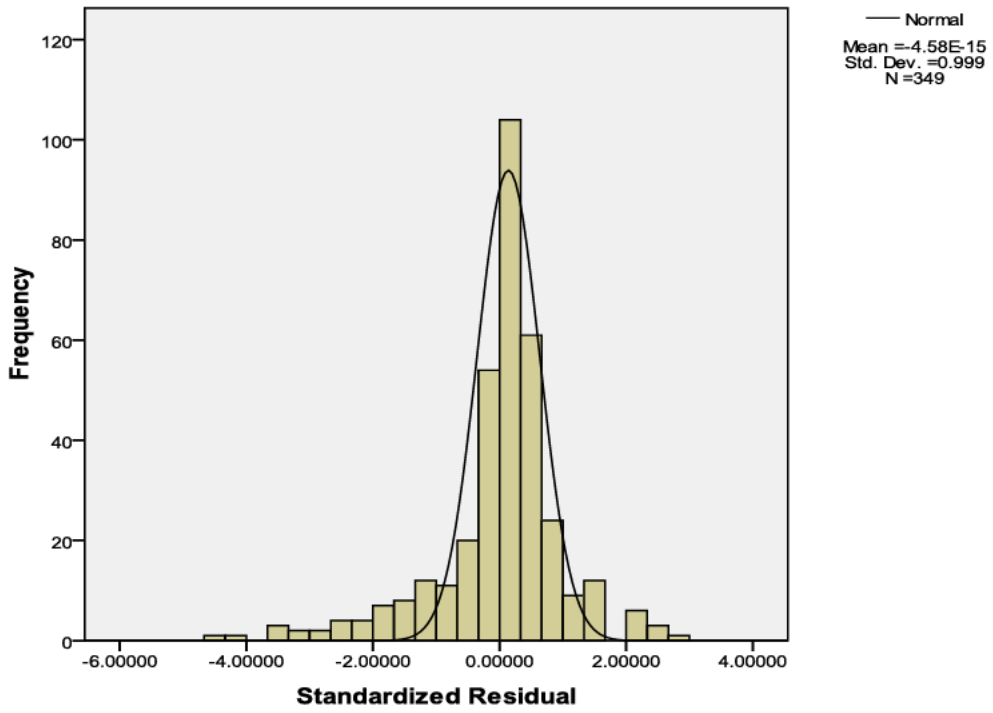


Figure 5.18: Test of Normality

5.8.3 Test of Linearity

One of the fundamental assumptions of regression is that there is a linear relationship between the independent variables and the dependent variable in order to avoid type I and type II errors. Hence, the linearity assumption of regression is assessed by determining if there is multi-collinearity amongst the independent variables. Multi-collinearity indicates a high correlation relationship amongst the independent variables, which does not indicate a good regression model. High correlation (r = 0.9 and above) amongst the independent variables is an indication of multi-collinearity (Pallant, 2011).

In this study, multi-collinearity was assessed through the tolerance value and variance inflation factor (Variance Inflation Factor) in a regression analysis. The tolerance value indicates how

much of the variability of the independent values is not explained by the other independent variables in the model. A value of tolerance below 0.10 indicates the presence of multi-collinearity, while VIF is an inverse of the tolerance value which should not be higher than 10 (Pallant, 2011). Since only one independent variable was regressed against a dependent variable on different occasions in this study and multi-collinearity exists in a situation where there is more than one variable, it was concluded that multi-collinearity is not a threat to the findings of the data analysis.

5.9 Reliability Test

Reliability analysis measures the internal consistency of the measurement instrument (Pallant, 2011). It indicates the consistency of the data collected by the survey questionnaire. Cronbach's alpha was computed to measure reliability in this study. According to Hair *et al*. (2010), a Cronbach's alpha score greater than or equal to 0.7 indicates a good reliability measure. As shown in Table 5.18, the result of the reliability measure reveals that the Cronbach's alpha result for all the constructs is above the 0.7 threshold, indicating good reliability amongst the items of the constructs. However, the item "I tend to ignore information security procedures that I think are not necessary" (EBI 04) was excluded from the measure since this improved reliability, and the question does not necessarily measure employees' behavioural intention. A one sample test was also conducted to measure the agreement/disagreement of the reliability test, and the result indicates significant agreement of the respondents with the reliability measure.

Table 5.18: Reliability Measure

Construct	Cronbach's Alpha	No. of Items
ISS	.901	5
NOB	.880	5
STA	.920	7
PEF	.894	6
PCB	.924	8
COD	.889	5
SOP	.914	6
EBI	.883	5

5.10 Influence of Compliance Rate on Experience of Information Security Breaches

This section presents the results of the Spearman's Rho correlation relationship between compliance rate and experience of information security breaches. The results of the correlation in Table 5.19 show that a positive significant relationship exists for all pairs of the variables. This means that a higher frequency in the one variable is associated with a lower frequency in the other variable, and vice visa. For example, the relationship between ISB01 and ISR01 shows rho = .351, p<.005; ISB03 and ISR01 (rho = 0.262, p< 0.005); and ISB03 and ISR03 (rho = 0.435; p < 0.005).

Table 5.19: Relationship between Compliance Rate and Experience of Information Security Breaches

			ISR01	**ISB01**	**ISR03**	**ISB03**
Spearman's rho	ISR01 How often does your organisation review its ISS Policy (ISSP) compliance?	Corr. Coeff.	1.000			
		Sig. (2-tailed)	.			
		N	348			
	ISB01 How often does your organisation experience information security breaches?	Corr. Coeff.	.351**	1.000		
		Sig. (2-tailed)	.000	.		
		N	348	355		
	ISR03 When last did your organisation adopt a new ISS Policy (ISSP)?	Corr. Coeff.	.380**	.239**	1.000	
		Sig. (2-tailed)	.000	.000	.	
		N	335	340	340	
	ISB03 When last did your organisation successfully avert a pending information security breach?	Corr. Coeff.	.262**	.272**	.435**	1.000
		Sig. (2-tailed)	.000	.000	.000	.
		N	331	337	326	337

**. Correlation is significant at the 0.01 level (2-tailed).

5.11 The Relationships Between Organisational ISSsPs and ISSsPs that Successfully Prevent Information Security Breaches

The study applied the Chi-square test to investigate if a significant relationship exists between the items of international standard policy. Fisher's test was also conducted to investigate if the conditions are violated. As shown in Table 5.20, the result of the cross-tabulation and Fisher's test indicates that there is a significant relationship between usage and successful usage of FISMA, p=.001. A significant number of respondents that work for banks that subscribe to FISMA indicated that it successfully prevents an information security breach. A significant relationship was also found between usage and successful usage of HIPAA, p = 0.001. In addition, the findings revealed a significant relationship between usage and successful usage of SOX, p<.0005. A significant number of those respondents employed by banks that subscribe to SOX indicated that it successfully prevents an information security breach; while a significant number who work for banks that do not subscribe to it indicated that it is their experience that security breaches are not prevented using this ISSsPs tool. Furthermore, the findings show that there is a significant relationship between usage and successful usage of ISO/IEC 17799 (p = 0.001), which means that using ISO/IEC 17799 successfully prevents an information security breach; while a significant number of respondents in banks that do not subscribe to ISO/IEC 17799 indicated that it is their experience that security breaches are not prevented using this ISSP. Finally, the findings revealed a significant relationship between usage of GLBA and successful usage of GLBA. This indicates that a significant number of respondents employed by banks that subscribed to GLBA indicated that it successfully prevents information security breaches.

Table 5.20: Cross-Tabulations Between ISSsPs Organisations Subscribed to and ISSsPs that Successfully Prevent Information Security Breaches

					Total	**Fisher's Exact Test**	
			Yes	**No**		**Exact Sig. (2-sided)**	**Exact Sig. (1-sided)**
FISMA	Yes	Count	9	39	48	.001	.001
		Expected Count	3.0	45.0	48.0		
		% within R2.1 FISMA	18.8%	81.3%	100.0%		
		Std. Residual	3.5	-.9			
	No	Count	13	294	307		
		Expected Count	19.0	288.0	307.0		
		% within R2.1 FISMA	4.2%	95.8%	100.0%		
		Std. Residual	-1.4	.4			

					Total	Fisher's Exact Test	
			Yes	No		Exact Sig. (2-sided)	Exact Sig. (1-sided)
HIPAA	Yes	Count	19	23	42	.000	.000
		Expected Count	4.5	37.5	42.0		
		% within R2.2 HIPAA	45.2%	54.8%	100.0%		
		Std. Residual	6.9	-2.4			
	No	Count	18	289	307		
		Expected Count	32.5	274.5	307.0		
		% within R2.2 HIPAA	5.9%	94.1%	100.0%		
		Std. Residual	-2.5	.9			
SOX	Yes	Count	58	70	128	.000	.000
		Expected Count	27.8	100.2	128.0		
		% within R2.3 SOX	45.3%	54.7%	100.0%		
		Std. Residual	5.7	-3.0			
	No	Count	19	208	227		
		Expected Count	49.2	177.8	227.0		
		% within R2.3 SOX	8.4%	91.6%	100.0%		
		Std. Residual	-4.3	2.3			
ISO/IEC 17799	Yes	Count	149	32	181	.000	.000
		Expected Count	113.0	68.0	181.0		
		% within R2.4 ISO/IEC 17799	82.3%	17.7%	100.0%		
		Std. Residual	3.4	-4.4			
	No	Count	67	98	165		
		Expected Count	103.0	62.0	165.0		
		% within R2.4 ISO17799	40.6%	59.4%	100.0%		
		Std. Residual	-3.5	4.6			
GLBA	Yes	Count	5	17	22	.000	.000
		Expected Count	1.4	20.6	22.0		
		% within R2.5 GLBA	22.7%	77.3%	100.0%		
		Std. Residual	3.1	-.8			
	No	Count	17	314	331		
		Expected Count	20.6	310.4	331.0		
		% within R2.5 GLBA	5.1%	94.9%	100.0%		
		Std. Residual	-.8	.2			

5.12 Contribution of Motivational Factors to Intention to Comply and Impact on Organisational Compliance

This section presents the results of the regression analysis which was conducted to determine the motivational factors and their effects on intention to comply with ISSsPs. The study first tested for the direct influence of the independent variables on employee behavioural intention and later, the effect of these variables on ISSsPs. It also included a multi-regression analysis which considered all the variables together in order to identify which strongly affects ISSsPs.

5.12.1 Effect of Normative Beliefs on Employee Behavioural Intention

This study used simple regression analysis to ascertain the effect of normative beliefs on employee behavioural intention in the Nigerian banking industry. The independent variable "normative beliefs" was regressed on the dependent variable "employee behavioural intention". The result of the regression model in Table 5.21 shows the value of regression coefficient R = .572, R^2 = .321, model's F (1, 347) = 168.461 and significance level P = 0.000, indicating that the model is significant at P < 0.05. In terms of the predictive effect of normative beliefs on employee behavioural intention in the Nigerian banking industry, the result of the R-square (R^2 = .321) indicates that normative beliefs of employees explained 32.1 % of the variance in employees' behavioural intention. The result also indicates a strong positive correlation relationship (β = .529, p < 0.05) between normative beliefs and employee behavioural intention. The correlation co-efficient implies that employee behavioural intention increases by 57.2%, if normative beliefs increase by 1. Hence, the finding revealed that normative beliefs are a significant predictor of employees' behavioural intention in the Nigerian banking industry.

Table 5.21: Effect of Normative Beliefs on Employees' Behavioural Intention

Model	**R**		**R Square**	**Adjusted R Square**	**Std. Error of the Estimate**	
1	.572[a]		.321	.327	1.10034	
Model		**Unstandardised Coefficients**		**Standardised Coefficients**	**T**	**Sig.**
		B	**Std. Error**	**Beta**		
1	(Constant)	2.856	.233		12.260	.000
	NOB	.535	.040	.584	12.979	.000
	Summary: F ratio: 168.461					

a. Predictors: (Constant)

b. Dependent Variable: EBI

5.12.2 Effect of Security Threat Awareness on Employees' Behavioural Intention

Simple regression analysis was used to ascertain the effect of security threat awareness on employee behavioural intention in the Nigerian banking industry. The independent variable "security threat awareness" was regressed on the dependent variable "employee behavioural intention". The results of the regression model in Table 5.22 show regression coefficient R = .664, R^2 = .440, model's F (1, 347) = 273.111 and significance level P = 0.000, indicating that the model is significant at P < 0.05. In terms of the predictive effect of security threat awareness on employees' behavioural intention in the Nigerian banking industry, the result of the R-square (R^2 = .440) indicates that security threat awareness of employees explained 44.0% of the variance in employees' behavioural intention in the Nigerian banking industry. The result also indicates a strong positive correlation relationship ($\beta = 0.721$, $p < 0.05$) between security threat awareness and employees' behavioural intention. The correlation co-efficient implies that employees' behavioural intention increases by 66.4%, if security threat awareness increases by 1. Hence, the finding revealed that security threat awareness is a significant predictor of employees' behavioural intention in the Nigerian banking industry.

Table 5.22: Effect of Security Threat Awareness on Employees' Behavioural Intention

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate				
1	.664[a]	.440	.439	.99333				
Model		**Unstandardised Coefficients**		**Standardised Coefficients**	**T**	**Sig.**	**Collinearity Statistics**	
		B	**Std. Error**	**Beta**			**Tolerance**	**VIF**
1	(Constant)	1.69	.254		6.680	.000		
	STA	.728	.044	.664	16.526	.000	1.000	1.000
	Summary: F ratio: 273.111							

a. Predictors: (Constant), STA
b. Dependent Variable: EBI

5.12.3 Effect of Perceived Effectiveness of ISSsPs Compliance on Employees' Behavioural Intention

Regression analysis was carried out to ascertain the effect of Perceived Effectiveness of IS Policy Compliance on employees' behavioural intention in the Nigerian banking industry. The independent variable Perceived Effectiveness of IS Policy Compliance was regressed on the dependent variable "employee behavioural intention". As shown in Table 5.23, the result of the regression model indicates the value of regression coefficient R = .664, R2 = .440, model's F (1, 347) = 273.111 and significance level P = 0.000, indicating that the model is significant

at P < 0.05 for the predictive effect of Perceived Effectiveness of ISSsPs Compliance on employees' behavioural intention in the Nigerian banking industry. The result of the R-square (R2 = .440) indicates that Perceived Effectiveness of ISSsPs Compliance of employees explained 44.0% of the variance in employees' behavioural intention in the Nigerian banking industry. The result also indicates a strong positive correlation relationship (β = 0.728, p < 0.05) between Perceived Effectiveness of ISSsPs Compliance and employees' behavioural intention. The correlation co-efficient implies that employees' behavioural intention increases by 66.4%, if Perceived Effectiveness of IS Policy Compliance increases by 1. Hence, the finding reveals that Perceived Effectiveness of ISSsPs Compliance is a significant predictor of employees' behavioural intention in the Nigerian banking industry.

Table 5.23: Effect of Perceived Effectiveness of IS Policy Compliance on Employees' Behavioural Intention

Model	**R**	**R Square**	**Adjusted R Square**	**Std. Error of the Estimate**
1	.664[a]	.440	.439	.99333

Model		**Unstandardised Coefficients**		**Standardised Coefficients**	**T**	**Sig.**	**Collinearity Statistics**	
		B	**Std. Error**	**Beta**			**Tolerance**	**VIF**
1	(Constant)	1.69	.254		6.680	.000		
	STA	.728	.044	.664	16.526	.000	1.000	1.000
	Summary: F ratio: 273.111							

a. Predictors: (Constant), PEF
b. Dependent Variable: EBI

5.12.4 Effect of Perceived Bias on Employees' Behavioural Intention

The effect of perceived bias on employees' behavioural intention in the Nigerian banking industry as seen in Table 5.24 was investigated using simple regression analysis. The independent variable "perceived bias" was regressed on the dependent variable "employee behavioural intention". As shown in Table 5.25, the result of the regression model indicates a regression coefficient R =.592 R^2 = .350, model's F (1, 347) = 186.677 and significance level P = 0.000, indicating that the model is significant at P < 0.05. The predictive effect of perceived bias on employees' behavioural intention in the Nigerian banking industry is indicated by the R-square score (R^2 =. 350), which indicates that perceived bias amongst employees explained 35.0% of the variance in employees' behavioural intention in the Nigerian banking industry. The result also indicates a strong positive correlation relationship (β = 0. 471, p < 0.05) between perceived bias and employees' behavioural intention. The correlation co-efficient implies that

employees' behavioural intention increases by 59.2%, if perceived bias increases by 1. Hence, the finding revealed that perceived bias significantly predicts employees' behavioural intention in the Nigerian banking industry.

Table 5.24: Effect of Perceived Bias on Employees' Behavioural Intention

Model	R		R Square	Adjusted R Square	Std. Error of the Estimate
1	.592[a]		.350	.347	1.08213

Model			Unstandardised Coefficients		Standardised Coefficients	T	Sig.
			B	Std. Error	Beta		
1	(Constant)		3.241	.195		16.613	.000
	PCB		.471	.034	.592	13.663	.000
	Summary: F ratio: **186.677**						

a. Dependent Variable: EBI

b. Predictor: (Constant), PCB

5.12.5 Effect of Certainty of Detection on Employees' Behavioural Intention

The effect of certainty of detection on employees' behavioural intention in the Nigerian banking industry was investigated using simple regression analysis. The independent variable "certainty of detection" was regressed on the dependent variable "employee behavioural intention". As seen in Table 5.25, the result of the regression model indicates a regression coefficient R = 0.568, R^2 = .322, model's F (1, 347) = 164.471 and significance level P = 0.000, indicating that the model is significant at P < 0.05. The predictive effect of certainty of detection on employees' behavioural intention in the Nigerian banking industry is indicated by the R-square score (R^2 = .322), which means that certainty of detection amongst employees explained 32.2% of the variance in employees' behavioural intention in the Nigerian banking industry. The result also indicates a strong positive correlation relationship ($\beta = 0.524$, $p < 0.05$) between certainty of detection and employees' behavioural intention. The correlation co-efficient implies that employees' behavioural intention increases by 56.8 %, if certainty detection increases by 1. Hence, the finding revealed that certainty of detection is a significant predictor of employees' behavioural intention in the Nigerian banking industry.

Table 5.25: Effect of Certainty of Detection on Employees' Behavioural Intention

Model	R	R Square	Adj. R Square	Std. Error of the Estimate		
1	.568[a]	.322	.320	1.08520		
Model		**Unstandardised Coefficients**		**Standardised Coefficients**	**T**	**Sig.**
		B	**Std. Error**	**Beta**		
1	(Constant)	2.886	.235		12.300	.000
	COD	.524	.041	.568	12.825	.000
Summary: F ratio: 164.471						

a. Predictors: (Constant), COD

b. Dependent Variable: EBI

5.12.6 Effect of Severity of Penalty on Employees' Behavioural Intention

Similar to the above, the study used simple regression to test for the effect of severity of penalty on employees' behavioural intention in the Nigerian banking industry. The independent variable "severity of penalty" was regressed on the dependent variable "employee behavioural intention". Table 5.26 shows that the findings of the regression model indicate a regression coefficient score R = .780, R^2 =.608, model's F (1, 346) = 535.904 and significance level P = 0.000, indicating that the model is significant at P < 0.05.

Table 5.26: Effect of Severity of Penalty on Employee's Behavioural Intention

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate		
1	.780[a]	.608	.607	.84053		
Model		**Unstandardised Coefficients**		**Standardised Coefficients**	**t**	**Sig.**
		B	**Std. Error**	**Beta**		
1	(Constant)	1.506	.190		7.926	.000
	SOP	.751	.032	.780	23.150	.000
	Summary: F ratio**: 535.904**					

a. Predictors: (Constant), SOP

b. Dependent Variable: EBI

The predictive effect of severity of penalty on employees' behavioural intention in the Nigerian banking industry is indicated by the R-square score (R^2 = .608), which indicates that severity

of penalty accounted for 60.8% of the variability in employees' behavioural intention in the Nigerian banking industry. The result also indicates a strong positive correlation relationship ($\beta = 0.751$, $p < 0.05$) between severity of penalty and employees' behavioural intention. The correlation co-efficient implies that an increment of 78% in employees' behavioural intention is explained by a single unit increment in severity of penalty. Hence, the significance level of $P < 0.05$ reveals that severity of penalty is a significant predictor of employees' behavioural intention in the Nigerian banking industry.

The subsequent sections report the results of the regression analysis which tested the influence of motivational factors on ISSsPs.

5.12.7 Effect of Normative Beliefs on ISSsPs Compliance

The findings on the effect of normative beliefs on ISSsPs were tested through regression analysis. The independent variable "normative beliefs" was regressed on the dependent variable "ISSsPs". Table 5.27 shows that the regression model indicated the value of regression coefficient $R = .692^a$, $R^2 = .470$, model's $F(1, 351) = 322.93$ and significance level $P = 0.000$, indicating that the model is significant at $P < 0.05$. The predictive effect of normative beliefs on ISSsPs in the Nigerian banking industry is indicated by the R-square score ($R^2 = .470$), which means that normative beliefs amongst employees accounted for 47% of the variability in ISSs in the Nigerian banking industry.

Table 5.27: Effect of Normative Beliefs on Organisational Compliance

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate		
1	.692[a]	. 479	.478	1.23372		
Model		**Unstandardised Coefficients**		**Standardised Coefficients**	**T**	**Sig.**
		B	**Std. Error**	**Beta**		
1	(Constant)	.875	.261		3.350	.001
	NOB	.819	.046	.692	17.970	.000
	Summary of F-ratio: **322.903**					

a. Predictors: (Constant), NOB

b. Dependent Variable: ISSsPs

The result also indicates a strong positive correlation relationship ($\beta = 0.819$, $p < 0.05$) between normative beliefs and ISSsPs. The correlation co-efficient implies that an increment of 69.2% in ISSsPs is explained by a single unit increment in normative beliefs. Hence, the significance level of $P < 0.05$ reveals that a normative belief is a significant predictor of ISSs in the Nigerian banking industry.

5.12.8 Effect of Threats Awareness on ISSsPs Compliance

The findings on the effect of security threat awareness on ISSsPs were also tested through regression analysis, with the independent variable "security threat awareness" regressed on the dependent variable "ISSsPs". Table 5.28 shows that the findings of the regression model indicate a value of regression coefficient $R = .669^a$, $R^2 = .447$, model's $F(1, 348) = 281.261$ and significance level $P = 0.000$, indicating that the model is significant at $P < 0.05$. The predictive effect of security threat awareness on ISSs in the Nigerian banking industry is indicated by the R-square score ($R^2 = .447$), which means that security threat awareness amongst employees accounted for 55.8% of the variability in ISSs in the Nigerian banking industry. The result also indicates a strong positive correlation relationship ($\beta = 0939$, $p < 0.05$) between security threat awareness and ISSs. The correlation co-efficient implies that an increment of 66.9% in ISSs is explained by a single unit increment in security threat awareness. Hence, the significance level of $P < 0.005$ reveals that security threat awareness is a significant predictor of ISSsPs in the Nigerian banking industry.

Table 5.28: Effect of Security Threat Awareness on ISSsPs

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.669[a]	.447	.445	1.26294

Model		**Unstandardised Coefficients**		**Standardised Coefficients**	**T**	**Sig.**
		B	**Std. Error**	**Beta**		
1	(Constant)	.135	.323		.418	.676
	STA	.939	.056	.669	16.771	.000
Summary of F-ratio: **281.261**						

a. Predictors: (Constant), STA

b. Dependent Variable: ISSsPs

5.12.9 Effect of Perceived Effectiveness of ISSsPs Compliance on ISSsPs

The finding on the effect of security threat awareness on ISSsPs was also tested through regression analysis in this study. Table 5.29 reveals that the independent variable "security threat awareness" was regressed on the dependent variable "ISSsPs". The findings of the regression model indicate the value of regression coefficient R = .669[a], R^2 = .447, model's F (1, 348) = 281.261 and significance level P = 0.000, indicating that the model is significant at P < 0.05. The predictive effect of security threat awareness on ISSsPs in the Nigerian banking industry is indicated by the R-square score (R^2 = .447), which means that security threat awareness amongst the employees provided 55.8% of the variability in information secure ty standards in the Nigerian banking industry. The result also indicates a strong positive correlation relationship (β = 0939, p < 0.05) between security threat awareness on ISSs. The correlation co-efficient implies that an increment of 66.9% ISSsPs is explained by a single unit increment in security threat awareness. Hence, the significance level of P < 0.005 in the finding reveals that security threat awareness is a significant predictor of ISSsPs in the Nigerian banking industry.

Table 5.29: Effect of Perceived Effectiveness of ISS Compliance on ISSsPs

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.669[a]	.447	.445	1.26294

Model		**Unstandardised Coefficients**		**Standardised Coefficients**	**T**	**Sig.**
		B	**Std. Error**	**Beta**		
1	(Constant)	.135	.323		.418	.676
	STA	.939	.056	.669	16.771	.000
Summary of F-ratio: **281.261**						

a. Predictors: (Constant), PEF

b. Dependent Variable: ISSsPs

5.12.10 Effect of Perceived Bias on ISSsPs

The findings on the effect of ISSsPs on perceived bias in the Nigerian banking industry were tested through regression analysis with the independent variable "ISS" regressed on the dependent variable "perceived bias" Table 5.30 Indicates a regression model with the value of regression coefficient R = .610[a], R^2 = .373, model's F (1, 348) = 206.687 and significance level P = 0.000, indicating that the model is significant at P < 0.05. The predictive effect of ISSs in

the Nigerian banking industry is indicated by the R-square score (R^2 = .373), which means that ISSsPs amongst employees explained 37.3% of the variability in perceived bias in the Nigerian banking industry. The result also indicates a strong positive correlation relationship (β = 0.621, p < 0.05) between Perceived bias and ISSsPs. The correlation co-efficient implies that an increment of 61.0 % in perceived bias is explained by a single unit increment in ISSs. Hence, the significance level of P < 0.005 reveals that ISSsPs is a significant predictor of perceived bias in the Nigerian banking industry.

Table 5.30: Effect of Perceived Bias on ISSsPs

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.610[a]	.373	.371	1.35761

Model		**Unstandardised Coefficients**		**Standardised Coefficients**	**T**	**Sig.**
		B	**Std. Error**	**Beta**		
1	(Constant)	2.052	.244		8.393	.000
	STA	.621	.043	.610	14.377	.000
Summary of F-ratio: **206.687**						

a. Predictors: (Constant), PCB

b. Dependent Variable: ISSsPs

5.12.11 Effect of Certainty of Detection on ISSsPs Compliance

The findings on the effect of certainty of detection on ISSsPs were also tested through regression analysis. The independent variable "certainty of detection" was regressed on the dependent variable "ISSsPs". Table 5.31 shows that the findings of the regression model indicate the value of regression coefficient R = .578, R^2 = .335, model's F (1, 348) = 174.267 and significance level P = 0.000, indicating that the model is significant at P < 0.05. The predictive effect of certainty of detection on ISSs in the Nigerian banking industry is indicated by the R-square score (R^2 = .335), which means that certainty of detection amongst employees accounted for 33.5% of the variability in ISSs in the Nigerian banking industry. The result also indicates a strong positive correlation relationship (β = .688, p < 0.05) between certainty of detection and ISSsPs. The correlation co-efficient implies that an increment of 68.9% in ISSsPs is explained by a single unit increment in certainty of detection. Hence, the significance level of P < 0.005 reveals that certainty of detection is a significant predictor of ISSsPs in the Nigerian banking industry.

Table 5.31: Effect of Certainty of Detection on ISSsPs

Model	R	R Square		Adjusted R Square		Std. Error of the Estimate
1	.578[a]	.334		.332		1.38743
Model		**Unstandardised Coefficients**		**Standardised Coefficients**	**T**	**Sig.**
		B	**Std. Error**	**Beta**		
1	**(Constant)**	1.599	. 299		5.345	.000
	COD	.688	.052	. 052	13.201	.000
Summary of F-ratio: **174.267**						

a. Predictors: (Constant), COD

b. Dependent Variable: ISSsPs

5.12.12 Effect of Severity of Penalty on ISSsPs

The findings on the effect of severity of penalty on ISSsPs were tested through regression analysis. The independent variable "severity of penalty" was regressed on the dependent variable "ISSsPs". Table 5.32 shows that the findings of the regression model indicate the value of regression coefficient R = .589, R^2 = .347, model's F (1, 347) = 184.784 and significance level P = 0.000, indicating that the model is significant at P < 0.05. The predictive effect of severity of penalty on ISSs in the Nigerian banking industry is indicated by the R-square score (R^2 = .347), which means that severity of penalty amongst employees provided 34.7% of the variability in ISSsPs in the Nigerian banking industry. The result also indicates a strong positive correlation relationship (β = .727, p < 0.05) between severity of penalty and ISSsPs. The correlation co-efficient implies that an increment of 58.9% in ISSsPs is explained by a single unit increment in severity of penalty. Hence, the significance level of P < 0.05 reveals that severity of penalty is a significant predictor of ISSsPs in the Nigerian banking industry.

Table 5.32: Effect of Severity of Penalty on ISSsPs

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate		
1	.589[a]	.347	.345	1.38622		
Model		**Unstandardised Coefficients**		**Standardised Coefficients**	**T**	**Sig.**
		B	**Std. Error**	**Beta**		
1	(Constant)	1.271	.313		4.057	.000
	SOP	.727	.053	.589	13.594	.000
	Summary of F-ratio: **184.784**					

a. Predictors: (Constant), SOP
b. Dependent Variable: ISS

5.12.13 Effect of Employees' Intention to Comply on ISSsPs Compliance

The findings on the effect of employees' behavioural intention on ISSsPs was tested through regression analysis, with the independent variable "intention to comply" regressed on the dependent variable "ISSsPs". The findings of the regression model indicate the value of regression coefficient R = .558, R^2 = .312, model's F (1, 347) = 157.199 and significance level P = 0.000, indicating that the model is significant at P < 0.05. The predictive effect of employees' behavioural intention on ISSsPs in the Nigerian banking industry is indicated by the R-square score (R^2 = .312), which means that employees' behavioural intention amongst employees provided 31.2% of the variability in ISSsPs in the Nigerian banking industry. The result also indicates a strong positive correlation relationship (β = .714, p < 0.05) between employees' behavioural intention and ISSsPs. The correlation co-efficient implies that an increment of 55.8% in ISSsPs is explained by a single unit increment in employees' behavioural intention. Hence, the significance level of P < 0.05 reveals that employees' behavioural intention is a significant predictor of ISSsPs in the Nigerian banking industry. This shows that EBI significantly predicts ISSsPs.

Table 5.33: Effect of Employees' Intention to Comply on ISSsPs Compliance

Model	R	R Square		Adjusted R Square		Std. Error of the Estimate
1	.558[a]	.312		.310		1.42169
Model		**Unstandardised Coefficients**		**Standardised Coefficients**	**T**	**Sig.**
		B	**Std. Error**	**Beta**		
1	**(Constant)**	1.277	.338		3.782	.000
	COD	.714	.057	.558	12.58	.000
Summary of F-ratio: 157.199						

a. Predictors: (Constant),COD

b. Dependent Variable: ISSsPs

5.13 Testing the Mediating Effect of EBI to Comply on ISSsPs Compliance

This section presents the results on the mediating effect of employees' behavioural intention to comply (EBI) on the relationship between the six motivating factors and ISSsPs compliance. In testing for the mediation effect, the initial effect of the motivating factors on ISSsPs was tested and all the motivating factors were found to be significant predictors of ISSsPs. Similarly, the effect of the motivating factors was tested on the mediating variable (EBI) and

they were also found to be significant predictors of the mediators. The results on the effect of the mediating variable (EBI) on ISS are presented in the next sections:

5.13.1 Testing the Mediating Effect of EBI to Comply on ISSsPs Compliance

Table 5.34 shows that the findings on the mediating effect of employees' behavioural intention on the relationship between severity of penalty and ISSsPs reveal a value of regression coefficient R = .609, R^2 = .371, model's F (2, 344) = 101.602 and significance level P = 0.000, indicating that the model is significant at P < 0.05. The predictive effect of EBI on ISSs in the Nigerian banking industry is indicated by the R-square score (R^2 = 371), which means that EBI amongst employees provided 37.1% of the variability in ISSs in the Nigerian banking industry. The result also indicates a strong positive correlation relationship (β = .321, 484 p < 0.05) between EBI and ISSsPs. The correlation co-efficient implies that an increment of 32.1%, in ISSsPs is explained by a single unit increment in EBI. Hence, the significance level of P < 0.05 reveals that EBI is a significant predictor of ISSs in the Nigerian banking industry.

Table 5.34: Mediating Effect of EBI on the Relationship between SOP and ISSsPs

Model		R	R Square	Adjusted R Square		Std. Error of the Estimate
1		.609[a]	.371	.368		1.36336
Model		**Unstandardised Coefficients**		**Standardised Coefficients**	**T**	**Sig.**
		B	**Std. Error**	**Beta**		
1	(Constant)	.790	.335		2.356	.000
	EBI	.321	.087	.251	3.684	.000
	SOP	.484	.084	.393	5.759	.000
Summary of F-ratio: **101.602**						

a. Predictors: (Constant), SOP, EBI

b. Dependent Variable: ISSsPs

In Table 5.35 a further step was taken to regress both EBI and SOP on ISSsPs. The result of the regression model revealed that R = .609, R^2 = 0.371, model's F (2, 344 = 188.854 and significance level P = 0.000, indicating that both the independent variable (SOP) and the mediating variable (EBI) are significant predictors of ISSsPs. Hence, it is concluded that EBI mediates the relationship between severity of penalty and information security. However, since both severity of penalty and employees' behavioural intention remain significant, it can be affirmed that employees' behavioural intention partially mediates between SOP and ISSsPs.

Table 5.35: Mediating Effect of EBI between SOP and ISSsPs

Model		R	R Square	Adjusted R Square		Std. Error of the Estimate
1		.609[a]	.371	.368		1.36336
Model		**Unstandardised Coefficients**		**Standardised Coefficients**	**T**	**Sig.**
		B	**Std. Error**	**Beta**		
1	(Constant)	.790	.335		2.356	.000
	EBI	.321	.087	.251	3.684	.000
	SOP	.484	.084	.393	5.759	.000
Summary of F-ratio**: 101.602**						

a. Predictors: (Constant), EBI, SOP

b. Dependent Variable: ISSsPs

5.13.2 Mediating Effect of EBI on the Relationship between COD and ISSsPs

The regression analysis to test the mediating effect of EBI on the relationship between COD and ISS revealed a regression model R = .0.638, R^2 = 0.404, model's F (2, 344) = 118.130 and significance level P = 0.000, indicating that both the independent variable (COD) and the mediating variable (EBI) are significant predictors of ISSsPs. Hence, the findings revealed that EBI mediates the relationship between certainty of detection and ISSs policies compliance. However, since both COD and EBI remain significant, it is affirmed that there is partial mediation of employee behavioural intention between certainty of detection and ISSsPs compliance. The purpose of the analysis is to test if the EBI mediation effect of the two variables from the result submitted in Table 5.36 indicates that a mediation EBI mediates between the two variable, but was found to be partial mediation.

Table 5.36: Mediating Effect of EBI on the Relationship between COD and ISSsPs

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate		
1	.638[a]	.407	.404	1.31198		
Model		**Unstandardised Coefficients**		**Standardised Coefficients**	**t**	**Sig.**
		B	**Std. Error**	**Beta**		
1	(Constant)	.371	.340		1.092	.276
	COD	.418	.065	.324	6.423	.000
	EBI	.471	.060	.396	7.848	.000
Summary of F ratio: 118.130						

a. Predictors: (Constant), EBI, COD

b. Dependent Variable: ISSsPs

5.13.4 Mediating Effect of EBI between PEF and ISSsPs

The results of the test on the mediating effect of EBI on the relationship between perceived effectiveness of ISSsPs and ISSsPs compliance are shown in Table. 5.37. The findings of the regression model revealed R = .683, R^2 = .467, model's F (2, 345) = 150.971 and significance level P = 0.000, indicating that both the independent variables (perceived effectiveness of ISSsPs and employees' behavioural intention) are significant predictors of ISSsPs compliance. Hence, the findings revealed that employees' behavioural intention mediates the relationship between perceived effectiveness of ISSsPs and ISSs policies compliance. However, the result indicates a partial but not full mediation effect of employees' behavioural intention between perceived effectiveness of ISSsPs and ISSsPs, since both perceived effectiveness of ISSsPs and employees' behavioural intention remain significant predictors of ISSs policies compliance. The reason for the analysis was to test if the EBI mediation effect of the two variables from the result submitted in Table 5.37 indicate that a partial mediation EBI mediates between the two variable, but was found to be partial mediation.

Table 5.37: Mediating Effect of EBI between PEF and ISSsPs

Model	R	R Square	Adjusted R Square		Std. Error of the Estimate	
1	.683[a]	.467	.464		1.24305	
Model		**Unstandardised Coefficients**		**Standardised Coefficients**	**t**	**Sig.**
		B	**Std. Error**	**Beta**		
1	(Constant)	-.273	.337		-.809	.419
	PEF	.242	.067	.190	3.608	.000
	EBI	.761	.074	.543	10.327	.000
	Summary of F-ratio: **150.971**					

a. Predictors: (Constant), EBI, PEF

b. Dependent Variable: ISSsPs

5.13.5 Mediating Effect of EBI on the Relationship Between STA and ISSsPs

The test of the mediating effect of EBI on the relationship between information security threat awareness and ISS policy compliance is shown in Table 5.38. The findings of the regression model revealed R = .467, R^2 = .683, model's F (2, 467) = 150.971 and significance level P = 0.000, indicating that both the independent variables (information security threat awareness and employee behavioural intention) are significant predictors of ISSsPs compliance. Thus, employees' behavioural intention mediates the relationship between information security threat

awareness and ISSs policies compliance. However, the result indicates a partial but not full mediation effect of employees' behavioural intention between information security threat awareness and ISSsPs since both information security threat awareness and employees' behavioural intention remain significant predictors of ISSsPs compliance. The purpose of the analysis is to test if the EBI mediation effect of the two variables from the result submitted in Table 5.38 indicate that a partial mediation EBI mediates the between the two variable, but was found to be partial mediation.

Table 5.38: Mediating Effect of EBI on the Relationship Between STA and ISSsPs

Model	R	R Square	Adjusted R Square		Std. Error of the Estimate	
1	.683[a]	.467	.467		1.24305	
Model		**Unstandardised Coefficients**		**Standardised Coefficients**	**t**	**Sig.**
		B	**Std. Error**	**Beta**		
1	(Constant)	-.273	.337		-.809	.419
	PEF	.242	.067	.190	3.608	.000
	EBI	.761	.074	.543	10.327	.000
	Summary of F-ratio: **150.971**					

a. Predictors: (Constant), EBI, STA

b. Dependent Variable: ISSsPs

5.13.6 Mediating Effect of EBI between PCB and ISSsPs

Similar to the above, the result of the regression analysis carried out to test the mediating effect of employee behavioural intention on the relationship between perception biases and information security compliance is shown in Table 5.39. It reveals a regression model R = .658[a], R^2 = .433, model's F (2,344) = 131.393 and significance level P = 0.000, indicating that both the independent variables (perception biases and employees' behavioural intention) are significant predictors of ISSs policies compliance. Thus, employees' behavioural intention mediates the relationship between perception biases and ISS policies compliance. However, the result indicates a partial but not full mediation effect of employees' behavioural intention between perception biases and ISS policies since both perception biases and employees' behavioural intention remain significant predictors of ISSs policies compliance.

Table 5.39: Mediating Effect of EBI between PCB and ISSsPs

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Durbin-Watson	
1	.658[a]	.433	.430	1.29376		
Model		**Unstandardised Coefficients**		**Standardised Coefficients**	**t**	**Sig.**
		B	**Std. Error**	**Beta**		
1	(Constant)	.785	.313		2.510	.013
	PCB	.390	.064	.305	6.061	.000
	EBI	.437	.051	.430	8.537	.000
Summary of F-ratio: 131.393						

a. Predictors: (Constant), EBI, PCB

b. Dependent Variable: ISSsPs

5.13.6 Exploratory Factor Analysis

Exploratory Factor Analysis (EFA) is one of the methods employed in the analysis of individual influences of all the items that make up a construct in a study. However, concerning the testing of the EFA, sample size is commonly a determining factor in the valley of decision, either to drop or accept an item. The occasion where an item is dropped indicates that such an item is less than the threshold value, according to Tabachnick and Fidell (2014). The authors suggest several factor loadings, but with the characteristics of the on-going research, factor loadings with a value of 0.50 are considered appropriate, which is in agreement with the study of Ma and Pearson (2005). Consequently, factor loadings above this value are considered accurate and are used for the framework. Principal component extraction via promax rotation is adopted in achieving the relevant eight factors (components). In order to ensure the suitability of the sample, Kaiser-Meyer-Olkin (KMO) and Bartlett's tests were carried out, as shown in Table 5.40 , 5.41 and 5.42 .

Table 5.40: KMO and Bartlett's Test

KMO and Bartlett's Test		
Kaiser-Meyer-Olkin Measure of Sampling Adequacy		.963
Bartlett's Test of Sphericity	Approx. chi-Square	13680.432
	df	1176
	Sig.	.000

Table 5.41: Factor Analysis

Rotated Component Matrix								
	Component							
	1	2	3	4	5	6	7	8
ISS01	.673							
ISS02	.606							
ISS03	.781							
ISS04	.658							
ISS05	.602							
NOB01		.583						
NOB02		.635						
NOB03		.544						
NOB04		.543						
STA03			.529					
STA05			.587					
STA06			.522					
STA07			.605					
PEF01				.552				
PEF02				.517				
PEF03				.562				
PEF04				.548				
PEF05				.584				
PEF06				.542				
PCB02					.554			
PCB04					.536			
COD01						.556		
COD02						.553		
COD03						.638		
COD04						.543		
COD05						.610		
SOP02							.520	
SOP04							.509	
SOP05							.575	
EBI01								.568
EBI02								.764
EBI03								.644
EBI05								.695
EBI06								.692
Extraction Method: Principal Axis Factoring								
Rotation converged in 5 iterations								

Table 5.42: Factor Analysis and Name of the Constructs

Rotated Component Matrix		
Component		
CODE	Construct name	Significance
ISS01	Information Security Standards and Policies Compliance	.673
ISS02		.606
ISS03		.781
ISS04		.658
ISS05		.602
NOB01	Normative Belief	.583
NOB02		.635
NOB03		.544
NOB04		.543
STA03	Information Security Awareness	.529
STA05		.587
STA06		.522
STA07		.605
PEF01	Perceived Effectiveness of ISSsPs	.552
PEF02		.517
PEF03		.562
PEF04		.548
PEF05		.584
PEF06		.542
PCB02	Perceived Bias	.554
PCB04		.536
COD01	Certainty of Detection	.556
COD02		.553
COD03		.638
COD04		.543
COD05		.610
SOP02	Severity of Penalty	.520
SOP04		.509
SOP05		.575
EBI01	Employees Behavioural Intention	.568
EBI02		.764
EBI03		.644
EBI05		.695
EBI06		.692

5.18 Chapter Summary

This chapter presented and analysed the data collected for this study. Reliability tests and descriptive analyses were conducted on the constructs. Furthermore, the various influences on the constructs were explored and the exploratory factor analysis to extract the significant constructs for the framework development was carried out, identified and reported. The results are summarised and discussed in the following chapter. It is equally important to note that there are numerous tables containing the analysis in this chapter, but some important values were extracted to avoid the voluminous content and to present a readable thesis. Appendix A presents the letter from the language editor and F the contained table for analysis.

CHAPTER SIX
DISCUSSION OF FINDINGS

6.1 Introduction

This study investigated the extent of Nigerian banks' compliance with information security policies and standards, as well as the role of motivational factors in employee intention to comply with them. The findings were presented in Chapter Five. The current chapter discusses the findings in the context of the research questions, research objectives and hypotheses. A detailed discussion corroborated by the literature is presented, while the relevant research questions in relation to the study are as follows:

- What is the Nigerian banks' rate of compliance with international information security standards and policies?
- Is there any influence of the compliance rate on the experience of perceived information security breaches?
- How do employee motivational factors contribute to their intention to comply with international information security codes and standards?

6.2 Discussion of the Findings

This section is divided into three parts based on the study's objectives. The first part discusses the rate and extent to which Nigerian banks have complied with international ISSsPs. Part Two discusses the findings on the influence of the compliance rate and experience of perceived information security breaches amongst Nigerian banks, while Part Three focuses on the findings on employees' motivational factors that contribute to bank employees' intention to comply with international ISSsPs.

6.3 Discussion of Objective One

"The rate and extent of Nigerian banks' compliance with international information security standards and policies"

To determine the extent to which Nigeria complies with ISSsPs, the question pertaining to the extent to which the banks comply with information security standard and policies was designed and administered to the respondents for their response. Such questions are:

1. How often does your organisation review its ISS Policies?

Based on the results in Table 5.3 and Section 5.5, it was noted that a high number of respondents acknowledged that Nigerian banks review their information security standards and policies at least once a year. This indicates that it is a yearly routine, which has become the culture of the banks. A minority of respondents acknowledged that they do review their standards and policies at least less than a year. Consequent upon the findings, the compliance of Nigerian banks in reviewing ISSsPs was established. This corroborates the guidelines of NITDA (2013), which set a minimum required review and audit standard that addresses the management, operational and technical aspects of protecting information systems management in Nigeria. The findings also revealed a moderate level of incorporation of ISSsPs policies compliance as a core value amongst Nigerian banks.

2. Which of the following international ISSsPs does your organisation subscribe to?

Further descriptive analysis was conducted on the subscription of Nigerian banks in relation to the type of ISSsPs. The result shows that Nigerian banks subscribe to FIMA, HIPAA, SOX, ISO/IEC 17799 and GLBA, but with a high preference for ISO/IEC 17799. This indicates that Nigerian banks understand the importance of information security standards and policies compliance, which is a means of preventing information security breaches and cybercrime, with the assurance that the contents of the standards are dutifully followed and applied appropriately. However, in terms of updating the standards and policies, which focuses on the determination of the last time of adoption of new standards in Nigeria banks, the question relating to standards adoption was asked and the responses of the respondents are discussed next.

3. When last did your bank adopt a new standard?

In relation to the results presented in Table 5.5, the highest number of respondents indicated that a new ISS policy had been adopted within the past six to twelve months. Nevertheless, such adoption takes place as the IT used in the banking industry changes. This finding is in line with minimum security requirements for national information and information systems, which requiresthat information in the corporate enterprise management system must be subscribed to as well as being updated. This is in line with National Information Technology Development Agency (2013).

Moreover, these questions are very important when investigating the degree of compliance with international standards. Consequent upon the responses of the respondents, it shows that the Nigerian commercial banks do review their standards once in a year, with the full subscription given by the banks to FIMA, HIPAA, SOX, ISO/IEC 17799 and GLBA. In addition, it was indicated that Nigerian banks had adopted a new standard within six months and twelve months previously, although the finding of the study revealed that Nigerian banks review their information security standards and policies at least once a year, which unequivocally shows that ISSsPs compliance forms part of their practices. This corroborates the declaration of the British Standards Institute CBN Report (2014), which showed that the Central Bank of Nigeria complies with ISO/IEC 27001, which has led to a commitment to maintaining ISSsPs compliance.

On the other hand, the compliance with ISO/IEC 27001 was applauded by the British Standards Institute. This was only given to the central bank and not to the generality of the commercial banks, as the latter still subscribe to ISO/IEC 17799 in spite of the modification from ISO/IEC 17799 to ISO/IEC 27001. However, taking a closer look at Nigeria, being a developing country, compliance with technology change is a bit low if compared to other developed countries of the world. Nevertheless, there is full compliance given to information security standards and policies (FIMA, HIPAA, SOX and GLBA). Unequivocally, the contents of these standards are adequate enough to provide useful information for combating information security breaches in the banking sector, with the inclusion of ISO/IEC 17799.

The discussion of this section has provided distinctive evidence in providing answers to the research question which stated that " *What is the extent of Nigerian banks' compliance with international information security codes and standards?"*

6.4 Discussion of Objective Two

"Determination of the relationship between compliance rate and experience of perceived information security breaches."

This study investigated the relationship between compliance rate and information security breaches experience. Responses from the bank employees related to information security breaches were analysed, focussing on the extent to which compliance with information security

has impacted security breaches, either positively or negatively. There are basically three questions in this section. The questions are coded with ISB 01, ISB 02 and ISB 03, as presented in Tables 4.12, 4.13 and 4.14 respectively, while the analysis is presented in Tables 5.6, 5.7, 5.8, 5.20 and Figures 5.7, 5.8 and 5.9.

The first question (ISB 01) asks: *"How often does your organisation experience information security breaches?*" The results shown in Table 5.6 and Figure 5.7, indicates that a majority of the Nigerian banks experience information security breaches at least once a year. This falls in line with the investigative study of Malik and Islam (2019) on the impact of cybercrimes on banks' performance, with the moderating role of employees' information security awareness. The finding stated that cybercrime incidents have a negative impact on organisational performance, but information security awareness weakens the negative impact of cybercrimes on organisational performance.

Furthermore, the second question (ISB 02) posits: *which of the following international ISSsPs, in your experience, successfully prevent an information security breach*? The result, as indicated in Tables 5.7, 5.21 and Figure 5.8, shows the descriptive analysis of international ISSsPs that successfully prevent information security breaches in the banking sector. In reference to this, a majority of the respondents declared that FISMA, HIPAA, SOX and GLBA prevent information security breaches, based on their experience: while it was also indicated that the contents of the standards provide guidelines that can be followed in ensuring the successful prevention of occurrences of information security breaches in the banking sector. However, much emphasis was placed on the significant usefulness and adoption of ISO/IEC 17799 in preventing information security breaches. In the same vein, the study by Lu and Koufteros (2019) cannot be neglected, as it also agreed that standards (ISO) go beyond the mere prevention of information security breaches but also involve practices to detect the threats and also avert the breaches.

The third question (ISB 03) asked: *when last did your organisation successfully avert a pending information security breach?* The result of this is presented in Table 5.8 and Figure 5.9. The outcome of the analysis shows that a pending information security breach was averted over a year ago. This corroborates the study by Shave *et al*. (2014), which echoed that regular aversion of information security breaches is important in order to prevent intruders from gaining access to the organisation's assets. The collective result of the analysis in Table 5.20

shows the relationship between information security compliance rates and information security breaches. Based on the findings of the analysis, it can be inferred that there is a significant relationship between information security compliance rates and experiences of perceived information breaches.

It is evident that Nigerian banks experience information security breaches and there are also pending information security breaches which are yet to be averted, despite the responses of the respondents that Nigerian banks subscribe to standards It is therefore necessary to adopt and comply with international standards in order to avert these pending information breaches, whilst more emphasis should be placed on the need to implement the guidelines provided by the standards amongst employees. In relation to the assertion of Malik and Islam (2019), there is a negative effect of cybercrime on the performance of the banking sector. It is of importance to note that compliance with information security reduces insider threats in the banking sector. Moreover, Mishra and Dhillon's (2017) study declares that employee negligence and failure to comply with their organisation's information security standards and policies often result in huge costs to the organisation, making it difficult to combat and reduce the rate of information security breaches. It is on this premise that this study considered the factors that can promote ISSsPs in the banking sector, as discussed in Section 6.5.

6.5 Discussion of Objective Three

"Motivational factors that contribute to banks employees' intention to comply with international ISSsPs and codes."

Theoretical studies have also examined employees' motivational factors (behavioural factors) in order to examine their intention to comply with ISSsPs. These motivational factors improve organisational compliance with information security standards and policies. It is equally believed that these factors reduce insider threats in the banking sector and consequently bring about a reduction in cybersecurity. Hence, such motivational factors are: normative belief, severity of penalty, certainty of detection, perceived effectiveness of ISSsPs, awareness of information security threats and perception biases. In order to bring clarity to the study, the mentioned factors are considered in line with the research questions, objectives and hypotheses. Section 3.7 of the study contains the designed questionnaires used to address the influence of these factors.

6.5.1 Influence of Normative Beliefs on Employees' Behavioural Intention

The study investigated the influence of normative beliefs on employees' behavioural intention using descriptive analysis after the designing and collection of data from employees in the banking sector. Five items are used to seek the opinions of the employee's base on their experience. The result of the descriptive analysis in Table 5.10 shows that there is agreement amongst the respondents that "it is important to them that co-workers see them as an ethical person; that co-workers believe they should comply with information security policy standards; complying with ISSsPs results from the superior assessing their work; co-workers believe that it is important to comply with information security policies and standards; and to their knowledge, the majority of employees comply with the organisation's IS security policies. Table 5.28 shows the direct influence of Normative Beliefs on ISSsPs. Furthermore, the results equally show that normative belief is a significant predictor of ISSs in the Nigerian banking industry. To investigate Normative Beliefs' influence on intention to comply with ISSsPs. The results of the regression analysis in Table 5.21 show the influence of normative beliefs on intention to comply. The finding indicates that normative beliefs have a positive influence on intention to comply with ISSsPs and is a predictor of intention to comply with information security standards and policies compliance.

Normative beliefs refer to the extent to which employees act on the basis of what other employees expect of them, or what the organisational standard/norms expected of them (Lin and Roberts, 2020). Normative beliefs also explained what is expected of them by other employees and the organisation, which thus improves bank employees' behavioural intention towards ISSsPs. This indicates that employees adhere to their organisation's belief systems with respect to ISSsPs.

Hypothesis One of this study posited that normative beliefs influence employees' behavioural intention. Evidence was found to support this hypothesis. This finding is in line with Lin *et al.*'s (2020) assertion that employees with high information security policy-related norms will be more likely to experience psychological benefits from complying with ISSsPs and will consider complying as rewarding. If an employee feels that "everybody in the organisation follows the organisation's ISSsPs" (descriptive norm), "everybody thinks it is wrong to violate the organisation's ISSsPs" (injunctive norm), and/or "their manager thinks it is wrong to violate the ISSsPs" (subjective norm), they will be more likely to believe that they are morally obligated to follow the ISSsPs (personal norm) (Yazdanmehr and Wang, 2016). Kaymaz (2020) also highlighted the importance of normative beliefs and showed that they can influence

ISSsPs compliance amongst employees. The author observes that employees are able to recognise reasonable and acceptable ISSsPs-related behaviour through their perception of the majority of their fellow workers' expectations. An employee who perceives that ISSsPs compliance is what the majority believes should be done is more likely to internalise ISSsPs compliance behaviour as part of their value system.

Siponen *et al*.'s (2014) exploratory study on employees' adherence to information security policies shows that normative beliefs positively and significantly affect employees' intention to comply with such policies. In the same vein, Guan and Hsu (2020) also found a positive significant effect of normative beliefs on employees' behavioural intention and suggested that top management and supervisors should clearly and explicitly state the importance of security compliance.

In addition, Chiu and Tan (2020) state that the joint presence of a conditional preference for conformity and the belief that other people will conform will produce an agreement between normative beliefs and behavioural intention. Similarly, Héroux (2020) asserted that a person's subjective norm is weighted by his or her motivation to comply with those referents that approve or disapprove of performing the behaviour. Hence, an employee who believes that certain referents will hold a positive subjective norm if he or she performs behaviour is motivated to meet their expectations. Furthermore, when an employee believes that the entire organisation will approve of his/her behaviour towards information security compliance, he/she tends to be more security conscious and have better behavioural intentions towards ISSsPs.

It is noted that employees are able to recognise reasonable and acceptable ISSsPs-related behaviour through their perceptions of the majority of their fellow workers' expectations. An employee who perceives that ISSsPs compliance is what the majority believes should be done is more likely to internalise ISSsPs compliance behaviour as part of their value system. It is obvious that behaviour regarding the constant practice of ISSsPs from the co-worker and superior have influence on the followers. TPB also provided a support for justification for this section. TPB explains the concept of social influence, which refers to changes that occur in an individual's feelings, thoughts and behaviour, giving rise to changes in their interactions with other individuals and groups of people. The managers and other superiors in the Nigerian banking sector should see ISSsPs as a regular practice since it is obvious that their followers are imitating their behaviour in terms of information security and standards compliance.

Employees in the organisation tend to imitate others, especially co-workers and the superior officer, regarding their compliance with ISSsPs. Employees in Nigerian banks will comply with standards and policies of the banks if the managers, co-workers and superior officers in particular are complying with the policies and standards regarding the information security of their organisation. As it stands, the supervisors in the banking sector are envoys to comply with the ISSsPs as this is noted to have a positive influence in reducing information security breaches. The result in relation to normative beliefs is in line with the TPB that aims to predict an individual's intention to engage in certain behaviour at a specific time and place. Having considered the results of the analysis with related literature to support it, it is obvious that the results had met the third research question which posits: *how do employees' motivational factors contribute to their intention to comply with international information security codes and standards and their impact on organisational compliance*? It also supported the objective which stated: "*to investigate employee motivational factors which contribute to bank employees' intention to comply with international information security codes and standards, and their impact on organisational compliance*. The First hypothesis has been achieved, which stated *that normative beliefs influence information security standards and policies compliance.* The result has shown a positive influence amongst the constructs.

The second motivational factors to be considered is information security threats awareness, which is discussed next.

6.5.2 The Influence of Information Security Threats Awareness on Employee Behavioural Intention

In order to conduct an examination of the influence of information security threats awareness on intention to comply, seven questions (in Table 4.6) emanated from the conceptualisation of the factor, which were subsequently answered by the respondents. The descriptive analysis of information security threat awareness shown in Table 5.11 reveals that the respondents clearly understood the implications of violating security policies; that they have education about information security threats; that information regarding security threats has been communicated to them; that they are aware of the programme on general information security threats; that information security training was included as part of their orientation; and that the supervisor updates them on changes to information security procedures.

A further analysis (Table 5.22) was conducted to test the influence of the threats awareness on intention to comply with information security standards and policies compliance, which was also hypothesised in Section 3.7 and subsequently analysed. The finding revealed that security threats awareness is a significant predictor of employees' behavioural intention in the Nigerian banking industry. This also indicated that an increase in employees' awareness of security threats affects their behavioural intention to comply with ISSsPs.

Security threat awareness indicates employees' knowledge or lack of understanding of security threats that can impact an individuals' perceptions of risk and their subsequent decisions. This study hypothesised that security threat awareness influences employees' behavioural intention to comply with ISSsPs. Regression analysis was conducted to determine the influence of security threat awareness on ISSsPs directly in Table 5.9. The result revealed a positive influence of security threat awareness on information security standard and policies compliance. The finding implies that a unit increase in employees' awareness of security threats affects their behavioural intention to comply with ISSsPs.

This finding is in line with Safa *et al.*'s (2016), which affirmed that improving employees' awareness of security-related issues will improve compliance behaviour. The authors suggested training and awareness campaigns as the best methods to increase the understanding of information security which accommodates the uniqueness of specific times. Training would also ensure that users are aware that they can be held liable for information security misconduct. Moreover, Logan (2020) asserts that security awareness training addresses the vulnerabilities associated with human behaviour. According to Cox (2012), employees will be more conscious of the need to comply with security standards if they have a clearer understanding of ISSsPs and the consequences of information security breaches. Koohang *et al*. (2020) showed that security awareness can improve employees' behavioural intention by enabling users to be more conscious of identifying potential security attacks. Behavioural factors to motivate individuals to change their security-related behaviours are important to promote safe and secure computing. The investigation into information security awareness has shown its importance in promoting information security standards and polices compliance amongst employees.

An employee who is aware and has the understanding of information security threats will likely comply with security standards and policies guiding customers' information and organisational assets. Employees can receive awareness through training or education with a follow-up by

management. Awareness of information security threats (construct) will benefit the study, as it is included in the framework.

The result of the investigation into information security threats awareness has equally provided the answer to the research question: *how do employee motivational factors contribute to their intention to comply with international information security policies and standards?* It moreover supports the objective of this study which asked: *to investigate employee motivational factors which contribute to bank employees' intention to comply with international information security codes and standards, and their impact on organisational compliance*.

6.5.3 The Influence of ISSsPs Effectiveness on Employees' Behavioural Intention

ISSsPs effectiveness was considered amongst the factors conceptualised to contribute to the intention to comply with the ISSsPs. The variable measured how employees perceive the effectiveness of complying with ISS policy in view of the benefits attached. There are six items in Table 4.4 that were used as a measure to predict whether ISSsPs effectiveness influences employees' behavioural intention, which also determines the influence of ISSsPs effectiveness on actual compliance, otherwise called perceived information security compliance. The descriptive analysis conducted to examine the influence of the perceived effectiveness of ISSsPs compliance on behavioural intention in Table 5.23 indicates a significant agreement amongst the respondents that "information security policy is effective in achieving the organisational goals for information security; information security policy helps to accomplish information security objectives; information security policy keeps the risk at a minimum; compliance with the requirements of the information security policy reduces security risks; compliance with the requirements of the ISSsPs secures infrastructure; and overall, information security policy is effective in securing information at this organisation". A further analysis was conducted to investigate the influence of the effectiveness of ISSsPs on ISSsPs through the regression analysis in Table 5.29. The regression analysis reveals a significant influence amongst the variables. This indicates that the perceived effectiveness of ISSsPs is a significant predictor of ISSsPs in the Nigerian banking industry. In the same vein, an investigation into the direct influence of the perceived effectiveness of ISSsPs on information security standards and policies compliance was done through regression analysis. The test reveals that the

perceived effectiveness of ISSsPs is a significant predictor of ISSsPs in the Nigerian banking industry.

The findings of this study are in line with Mutimukwe *et al*.'s (2019) which found that when individuals perceive that compliance with information security standards and policies is effective within an information security context, they demonstrate favourable behaviour towards securing a computing environment. The authors further asserted that perceived effectiveness in an individual has a positive effect in securing the computing environment, particularly the internet. The situation is similar with regard to ISSsPs compliance. The PMT posits that behavioural intentions are influenced by a person's assessment of the likelihood that the behaviour will yield the expected outcome, as well as subjective evaluation of the risks and benefits of the outcome. An employee who believes that his/her actions will make a difference in securing information will be more likely to exhibit behaviour that is inclined to comply with ISSsPs. This position is supported by Heralth and Rao's (2009) study on 'Encouraging information security behaviours in organisations'. The study found that the perceived effectiveness of their actions plays an important role in employees' security policy compliance intentions. Moreover, the effectiveness of ISSsPs is taken into consideration while complying with it. In the same breadth, a research study conducted by Williams *et al*. (2019) that focused on how motivational factors influence information security standards and policies compliance shows that the effectiveness of ISSsPs has a positive influence on information security standards and policies compliance amongst employees.

In employing an antidote to any problem, the positive effect of the past event will likely influence individuals to do it again, having noticed the positive effect on the problems to be solved. In clear terms, employees in Nigerian banks complied with the ISSsPs based on their experiences regarding the effectiveness of ISSsPs. In relation to previous studies, it is noted that information security compliance reduces insider threats and shows that international standards and policies are effective when dutifully followed. Based on the results shown in Table 5.30, it can be agreed that the conceptualisation of the effectiveness of ISSsPs on intention to comply with ISSsPs has provided answers to the research question which stated: "*how do employee motivational factors contribute to their intention to comply with international information security policies and standards?"* The Effectiveness of ISSsPs is amongst the factors conceptualised and the result has shown a significant influence on the

ISSsPs. Besides, the result has equally supported the objective of this study which stated: "*To investigate employee motivational factors which contribute to bank employees' intention to comply with international information security policies and standards, and their impacts on organisational compliance".* Furthermore, the finding of the study is in line with the results of the hypothesis in Section 3.7 that posits that the effectiveness of ISSsPs influences international information security standards and policies compliance. It is therefore evident that in Nigerian banks, employees will comply with ISSsPs if they discover that compliance with ISSsPs can reduce insider threats and in turn reduce cybercrime.

6.5.4 Influence of Perception Bias on Employees' Behavioural Intention to Comply

In relation to the investigation into the influence of perceived bias on behavioural intention to comply with ISSsPs, the concepts of the hypothesis, objective and the research question were taken into consideration. Table 4.6 shows the eight items designed to measure perception bias based on the respondents' perceptions. In addition, Table 5.13 presents the descriptive analysis of the perception bias. The outcome of the analysis reveals that there is significant agreement amongst the respondents that, "in case of an information security threat, they always act swiftly no matter the severity of the threat; that the measures in place to counteract information security threats are suitable and work successfully; the measures used to counteract information security threats can successfully deal with the most complex of threats; the security-resisting mechanisms in place are successful in counteracting most threats that we experience; if unsure about a possible security threat, they prefer to take swift preventative measures rather than ignoring it and have to fix it after it has happened; the organisation sets high standards for the protection of its information assets; and overall, compliance with the information security policy at this organisation is good and the policies in place regarding information security are adequate to address security threats". Further analysis was conducted to strengthen the investigation into the influence of perceived bias on intention to comply with the ISSsPs. Section 5.12.4 and Table 5.25 present the outcome of the simple analysis. Findings revealed that perceived bias significantly predicts employees' behavioural intention to comply with ISSsPs in the Nigerian banking industry. Besides, based on the direct influence of perception bias on ISSsPs in Table 5.31, the result equally reveals that ISSsPs is a significant predictor of perceived bias in the Nigerian banking industry. Consequently, significant evidence was found to support a positive effect of perception biases on employees' behavioural intention.

In any organisation, every employee takes a different approach to decision-making by applying different strategies, considering different elements of the problem or assigning different values to options. The sixth hypothesis of the study was on the perception biases which significantly influence employees' behavioural intention to comply with ISSsPs. Thus, employees' perception biases will increase their behavioural intention. There is therefore a corroboration between the finding of this study and the study of Usher *et al*. (2019), in which the authors stated that employees' perceptions or judgement of a situation depends on whether the situation occurs consistently or inconsistently, which may thus influence their behaviour.

The influence of perceived bias finding supported by self-efficacy theory which posits that perceived biases influence the choices an individual makes, as well as the courses of action they adopt. People are more likely to perform a task if they perceive that they have the ability to do so and have confidence in their capacity. In establishing the results of the study in relation to the perceived bias, reference is made to Rodrigues (2020) who investigated the role of optimistic bias behaviour with the theory of planned behaviour. The author evaluates the influences on employees' intention to conduct safe handling behaviours in Brazil and the United States. The results suggested that perceived behavioural control and optimistic bias did not significantly influence behavioural intention in Brazil; while in the United States, optimistic behaviour has influence on the perceived behaviour. However, the overall result suggested that perception bias can contribute to predicting engagement in safe handling behaviours regarding information system. The submission of this study agreed that perception biases have positive influence on the intention to comply with ISSsPs. The submitted result of this study agreed with the hypothesis stated in section 3.8 that: "*perception bias influences information security standards and policies compliance"*. The result has equally provided an answer to the research question that posits: "*How do employee motivational factors contribute to their intention to comply with international information security codes and standards?"* The study has achieved the objective as posited: "*To investigate employee motivational factors which contribute to bank employees' intention to comply with international information security policies and standards".* With the result submitted, it is evident that employees in Nigerian banks will probably comply with ISSsPs, putting their perception into consideration. In developing the framework, perceived bias will be included, since the result shows a significant influence on international information security standards and policies compliance.

6.5.5 Influence of Certainty of Detection on Employees' Behavioural Intention to Comply

In relation to the investigation into the influence of certainty of detection on employees' behavioural intention to comply with ISSsPs, a descriptive analysis was employed. There are five items designed for this construct, as conceptualised in Figure 3 and in Table 4.2. The result of the descriptive analysis, as shown in Table 5.14, reveals significant agreement amongst the respondents that, "their computer practices are properly monitored for policy violations; any employees violating organisational security policies are most likely be caught; their computers are monitored for security threat exposure at random times; they are often assessed for information security compliance; and their computer is routinely checked for security threats at regular intervals". In strengthening the results exhibited in Table 5.14, the study further conducted simple regression analysis in Section 5.2.5 and Table 5.25. Moreover, the findings revealed that certainty of detection is a significant predictor of employees' behavioural intention in the Nigerian banking industry. Besides, the direct influence of certainty of detection on ISSsPs was also conducted through regression analysis. The result further indicates that certainty of detection is a significant predictor of ISSsPs in the Nigerian banking industry.

Certainty of detection is an important aspect of information security policies compliance. It refers to the certainty that an employee who does not comply with ISSsPs will be caught. In testing the study's hypothesis of the construct, the researcher stated that an employees' intention to comply with ISSsPs is influenced by certainty of detection. The result shows that a unit increase in certainty of detection of an employee who misbehaves regarding ISSsPs will significantly improve employees' behavioural intention to comply with ISSsPs.

Perceived vulnerability to potential security threats, employees' attitudes, social norms and certainty of detection all had a significant and positive effect on employees' intention to comply with information security policies. Intention to comply also had a significant effect on actual compliance (Koranteng *et al*., 2020).

This finding is in line with Raddatz *et al*.'s (2020), which declared that there was a positive effect of certainty of detection on security behaviour intention. If employees perceive that there is a high likelihood of being caught violating security policies, they are more likely to follow

such security policies. It can thus be concluded that certainty of detection is an effective way of shaping employees' security behaviour. This also corroborates the findings of Williams *et al*.'s (2019) study, which investigated the influence of motivation factors on information security policies and found that certainty of detection has a positive effect on information security policies amongst Nigerian banks. In addition, a study conducted by Jaynes and Loughran (2020) has given similar support to the submission of this study which stated that perceived certainty of apprehension is a more effective deterrent than the severity of sanctioning. Besides, in a similar examination into motivational factors that influence security behaviour, scholars have discovered that formal sanctions, threat appraisals, detection certainty, punishment certainty and severity play a crucial role in ISSsPs compliance intention, all of which are in conformity with the studies of Cheng *et al*. (2013) and Safa *et al*. (2019).

Drawing from all the results of this construct and the support from past studies, this has submitted an answer to the research question which stated: "*How do employee motivational factors contribute to their intention to comply with international information security standards and policies*?", while the objective "*To investigate employee motivational factors which contribute to bank employees' intention to comply with international information security standards and policies"* has been achieved. The hypothesis has also been met, which posits that *certainty of detection influences information security standards and policies compliance.*

6.5.6 Severity of Penalty and Employees' Behavioural Intention to Comply

This study also investigated the influence of the severity of penalty on employees' behavioural intention to comply with ISSsPs in the Nigerian banking industry. This was tested using descriptive analysis. As conceptualised in Figure 4, the factor contained six items designed for the purpose of getting responses from the respondents. Section 5.7.7 and Table 5.15 indicate the results of the descriptive analysis that was conducted. The result reveals a significant agreement amongst respondents that, "employees caught violating security policies are appropriately corrected; information security policies are enforced by punishing employees that break them; serial information security offenders amongst employees are appropriately disciplined; employees who repeatedly break security rules can lose their jobs; if they were caught violating organisational information security policies, they would be severely punished; and their employer takes strict action against any violation of information security policy". A

further test was conducted with the use of simple regression analysis to examine the influence of severity of penalty on employees' intention to comply in table 2.6. The result showed that severity of penalty is a significant predictor of employees' behavioural intention in the Nigerian banking industry.

Penalties affect people's decisions on whether or not to commit a crime. Pahnila *et al*. (2007) assert that imposing penalties for non-compliance with IS policies increases security behaviour. The severity of the penalty meted out for a security breach can influence employees' intention to comply with the security standard (Best, 2014). Hypothesis six of this study posited that the severity of the penalty meted out to employees will significantly influence their behavioural intention to comply with ISSsPs. The regression analysis showed a significant positive correlation between the severity of penalty on employees' behavioural intention to comply with ISSsPs. The result implies that a unit increase in severity of penalty meted out to employees for non-conformance with ISSsPs will improve employees' behavioural intention to comply with ISSsPs.

Meting out penalties to every staff member that errs in their actions or in conforming to rules is the practice of Nigerian banks, which has made the results of this study corroborate that of D'Arcy *et al*. (2009), who reported that personnel's misuse of information systems is influenced by the perceived severity of sanctions. In addition, Merhi and Ahluwalia (2019) asserted that the punishment factor influences the resistance to information systems security, while Baik (2017) and Brown (2017) found that the severity of penalty (sanctions) had a negative impact on security behaviour intentions. Additionally, the finding of this study is in line with the PMT that suggests that if a breach takes place as a result of an employee revealing passwords and this leads to problems for him/her and the organisation, he/she will not exhibit such behaviour in future.

It is however evident that the severity of penalty meted out to employees who violate information security standards positively influence ISSsPs. Although studies on the severity reveal that the punishment meted on the offenders who violate ISSsPs does not yield a good result by prompting them to comply with the standards, in Nigeria's concept, punishing the violator will make the other employees comply with the ISSsPs. This factor will be integrated into the framework since it is a positive predictor of the employees' compliance in Nigerian banks. As hypothesised in section 3.7, the result has justified that severity of penalty influence

on ISSsPs. Secondly, the research question has been answered, which posits: "*How do employee motivational factors contribute to their intention to comply with international information security standards and policies?*

6.5.7 Intention to Comply with ISSsPs

The intention to comply is a conceptualised variable to influence ISSsPs, as seen in Figure 3.6. The purpose is to find the influence of the intention to comply on ISSsPs. To determine this, there are six items presented in this construct and the collected data was analysed using descriptive analysis. The result of the descriptive analysis of EBI showed that the employees in Nigerian banks agreed to "protecting information and technology resources according to the requirements of the ISSsPs of the organisation; carrying out responsibilities as prescribed in the ISSsPs in order to ensure the security of the information; complying with information security procedures is their intention; they do ignore IS procedures that they think are not necessary; and they all have an intention to follow organisational security policies wherever possible and intention to comply with information security policies".

In order to test the influence of employees' behavioural intention on ISSsPs, a further regression analysis was conducted in table 5.33. The finding indicated that employees' intention is a significant predictor of ISSsPs in the Nigerian banking industry, of which there is a corroboration between this study and the declaration of Kim *et al*. (2014). Taking a clue from the authors, there was an assertion that users' attitude will determine their intention to use security measures to protect information. In addition to that, Siponen *et al*. (2014) developed a multi-theory based framework that explained employees' adherence to security policies, which also supports the claims of this study. The authors came out with the fact that intention to comply has a positive influence on the actual compliance (ISSsPs), after giving consideration to a conglomeration of elements from the protection motivation theory, the theory of reasoned action and the cognitive evaluation theory in Finland.

In this context, intention to comply is very important in predicting the actual compliance (ISSsPs) amongst the Nigerian banks. This also indicates that employees in Nigerian banks will likely comply with ISSsPs if there is an intention and willingness to do so. This motivator (EBI) is integrated into the framework since the result has shown that the intention to comply is a predictor of ISSsPs.

In summary, this study has investigated the motivational factors (normative belief, certainty of detection, awareness of information security threats, perceived bias, perceived effectiveness of ISSsPs) and found that all them are are predictors of compliance with ISSsPs.

Therefore, it is imperative to develop a framework to enhance the information security standards and policies compliance amongst Nigerian banks, as it is noted that compliance behaviours reduce information security threats in the application of the model. It is essential that each employee is aware of his responsibilities as defined in the model, coupled with the fact that the management of the banks in Nigeria enforce the rules. The usage of the framework spans through the normative belief, awareness of information security threats, certainty detection, effectiveness of ISSPS, perceived bias and intention to comply.

6.6 The Mediating effect of EBI on the Relationship between Motivational Factors and ISSsPs Compliance

In assessing the mediating effects of employees' behavioural intention on the relationship between motivational factors and employee compliance, the effect of the motivating factors was tested and all the factors were found to be significant predictors of ISSsPs. Similarly, the effect of the motivating factors was tested on the mediating variable (EBI) and they were also found to be significant predictors of the mediators. Hence, the results of the mediating hypotheses of EBI in this study all showed empirically significant mediating effects of EBI between the motivational factors and ISSsPs compliance amongst Nigerian banks.

Therefore, evidence was found to support the claim that employee behavioural intention mediates the relationship between the motivational factors of employees' compliance and ISSsPs. More specifically, the findings revealed that the effect of all the dimensions of motivational factors of employees' compliance on employees' behavioural intention to comply remains significant, indicating that there is a partial mediating effect of the motivating factors on the relationship between employees' behavioural intention and ISSsPs compliance.

This study employed the widely used procedure proposed by Baron and Kenny (1986). This procedure for supporting significant mediating effects suggests that the motivational factors (independent variable) of employee compliance must account for variations in ISSsPs compliance (dependent variable) when not controlling for employees' behavioural intention (mediator). The results of the analysis revealed that the condition is successfully achieved for each motivational factor in this study ($p < 0.05$). In addition, employees' behavioural intention

(mediator) significantly explained the variations in ISSsPs compliance (dependent variable). Furthermore, the motivational factors (independent variables) significantly accounted for the variations in employees' behavioural intention. Since both motivational factors and employees' behavioural intention remain significant, it is affirmed that all the dimensions of motivational factors have partial mediation effects between employees' behavioural intention and ISSsPs compliance. The findings on the mediating effect underscore the important role played by behavioural intention in employees' security compliance behaviour amongst Nigerian banks.

6.7 Summary of the Findings

This study investigated the extent of Nigerian banks' compliance with information security policies and standards, and the role of motivational factors in employees' intention to comply with ISSsPs. It also examined the direct relationship between compliance rate and the experience of information security breaches; as well as the effect of the dimensions of motivational factors to comply (severity of penalty (SOP)), certainty of detection (COD), normative beliefs (NOB), security threat awareness (STA), perception bias (PCB) and perceived effectiveness of employees' information security compliance (PEF) on employees' behavioural intention to comply with information security in Nigerian banks. Twelve hypotheses were developed to represent the mediating effect of EBI between the motivating factors to comply and information security policy compliance. The results showed the partial mediating effects of employees' behavioural intention between the motivating factors to comply and ISSsPs compliance. The findings revealed that all the motivating factors highlighted in this study are significant predictors of employees' behavioural intention in Nigerian banks. In addition, evidence was found to support the six hypothesised mediating effects of employee's behavioural intention to comply with security standards and the motivating factors to comply. Based on the outcomes of the study, the next chapter presents the design of the framework as suggested in Section 1.5.

CHAPTER SEVEN
DEVELOPMENT AND VALIDATION OF FRAMEWORK FOR INFORMATION SECURITY STANDARDS AND POLICIES COMPLIANCE

7.1 Introduction

Previous chapters concentrated on the analysis, results and discussion of the findings in relation to the quantitative strand of the study. This chapter concentrates on the development and validation of an employee compliance framework that highlights the compliance behaviour with information security standards and policies. The description of the framework, based on the influences of the individual factors on employees' intention to comply with information security standards and policies, the validation process and the selection criteria of experts are given. The chapter concludes with a summary which encompasses all the steps that were taken in the framework processes.

7.2 Framework Development

Here the fourth research question (Section 1.4) is answered in the context of Nigerian banks by developing an employee compliance framework based on the research findings and past studies. Hence, the following seven steps were taken to bring about the actualisation of the framework. Figures 7.1 to 7.8 show the processes involved in the development of the framework, while the fully developed framework is shown in Figure 7.9. The framework for the Nigerian banking sector encompasses motivational factors that promote employees' compliance with international information security standards and policies. The operationalisation and the contents of the framework informs the management in Nigerian banks of the factors that motivate employees to comply with ISSsPs, since research has shown that information security standards and policies provide useful information for combating insider threats and consequently reduce cybercrime. This framework is capable of reducing information security issues when the steps and the contents are dutifully followed by employees and enforced by management.

To achieve the objectives of this study, a quantitative approach explored individual banks regarding compliance, as well as the identification of the factors that promote information security standards and policies compliance. In developing the framework, exploratory factor analysis was carried out through SPSS, as shown in Table 5.42. The EFA extracted those

factors that are significant based on the factor loading value as shown in the table. Consequent to the EFA, some items which were not significant (falling below 0.5) were dropped and those that are significant (0.5 and above) are used for the framework development. The process of the framework development of this study is in line with the study conducted by Williams (2019). The author extracted the significant factors from multiple factors after the exploratory factor analysis.

Further explanations on how individual motivational factors are related to the employee's intention to comply using the significant items are provided, while the interaction between the employees' intentions to comply and actual compliance is expatiated.

7.3 Steps for Framework Development

7.3.1 Normative Belief

Table 5.42 contains the significant items of normative belief. The EFA was used to determine which of the items is fit for the framework and consequently answered the research question in Section 1.4, normative belief being amongst the listed motivational factors. Furthermore, Table 4.3 shows the number of items arrogated to the normative belief, of which the initial items were five. After the EFA, four significant items were retained and these items were shortened in phrases for the purpose of the framework development in Figure 7.1.

Following the results of the analysis, normative belief has a significant influence on employees' behavioural intention to comply with ISSsPs, which has made the factor fitfor the model. However, the result of the finding corroborates Kaymaz's (2020), whose study declared that normative belief has a positive effect on intention to comply with information security policies. In addition, the study by Guan (2020) cannot be jettisonedas it affirmed that normative belief, as well as continuance commitment, have a native influence on information security compliance.

Normative belief is a very important factor in promoting compliance with ISSsPs, as employees will likely comply with standards and policies if the norms of the organisation are stated clearly. Besides, employees' normative belief stated that when others are complying with ISSsPs, particularly superior officers or co-workers, employees will likely follow. This is as shown in Figure 7.1

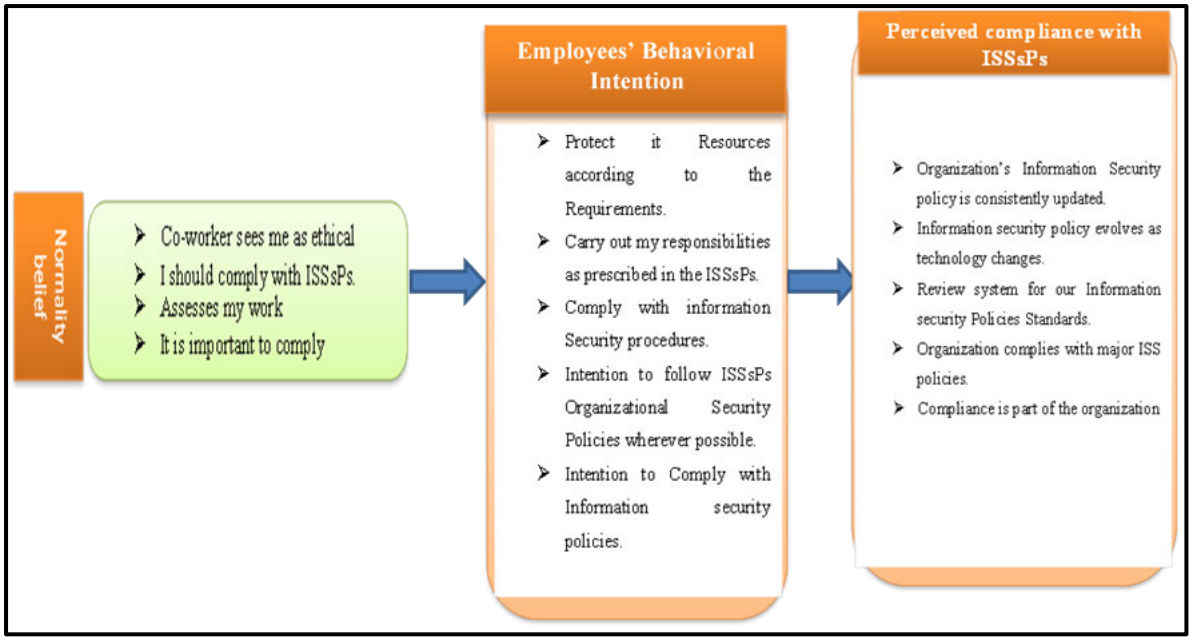


Figure 7.1: Normative Belief Influences Intention to Comply with ISSsPs
(Source: Author's Own)

7.3.2 Severity of Penalty

Table 5.42 contains the significant items of severity of penalty. The EFA was used to determine which of the items is fit for the framework and consequently answered the research question in Section 1.4, severity of penalty being amongst the listed motivational factors. Furthermore, Table 4.1 shows the number of items arrogated to the severity of penalty, of which the initial items were six. After the EFA, three significant items were retained and these items were shortened in phrases for the purpose of the framework development in Figure 7.2. These include: punishing employees that break IS; breakers of IS and rules lose their jobs; and violating ITSEC is severely punished.

The study is in conformity with Opoku-Ware and Apau (2020), who examined the effects of certainty of detection and severity of punishment on attitude towards compliance and also ISSP compliance behaviour through the lens of deterrence theory. The authors found that severity of punishment has a positive effect on attitude towards compliance behaviour. This has underpinned the inclusion of this factor in the framework. In this regard, the sanction given to employees who violate the information security of the banks should be severe, which may likely make them comply with ISSsPs, and further serves as a deterrent to other employees. Moreover, the element (severity of penalty) is considered to be good enough in promoting employees' compliance with international information security standards and policies in

Nigeria's banking sector. Therefore, it will be a better choice for the Nigerian banks to impose sanctions on those who violate ISSsPs. Discussed in the next section is the certainty of detection.

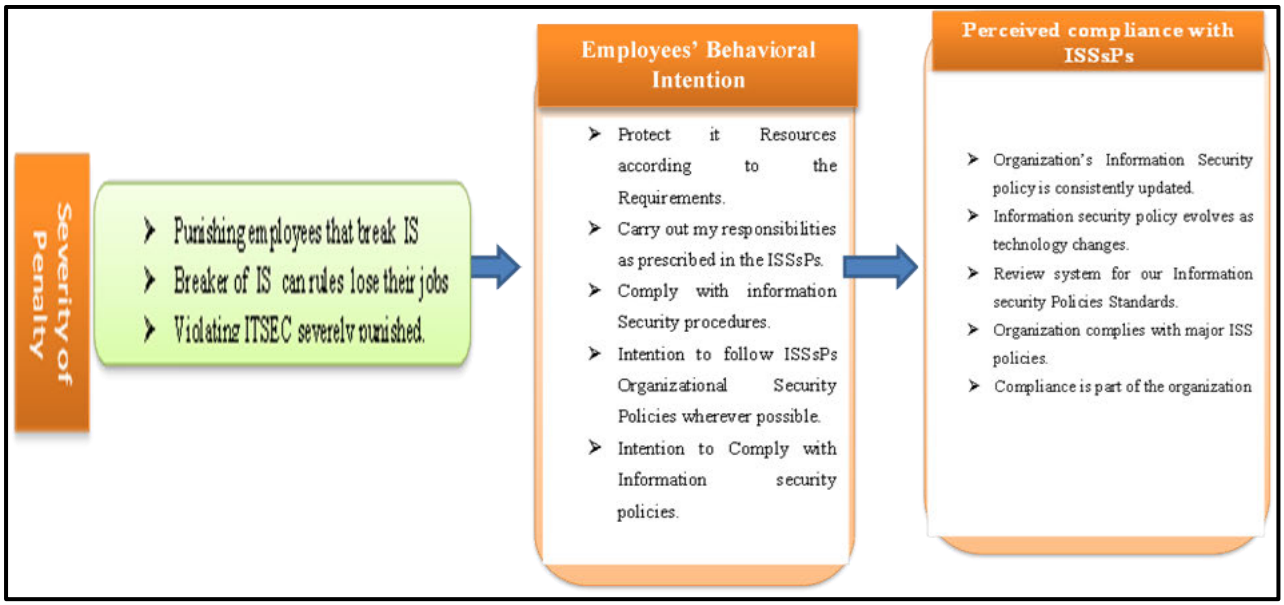


Figure 7.2: Severity of penalty influencing ISSsPs (Source: Author's Own)

7.3.3 Certainty of Detection

Certainty of detection contained five items, as shown in Table 4.2. With the EFA carried out, all the items still remained significant. They include: My computer practices are properly monitored for policy violations; if I violate organisational security policies, I will most likely be caught; my computer is monitored for security threat exposure at random times of which I am unaware; I am assessed for information security compliance; and my computer is routinely checked for security threat exposure at regular intervals. Consequently, all the items are integrated into the framework, as shown in Figure 7.2.

Going by the study and conclusion of Raddatz *et al*. (2020), there is a positive effect of certainty of detection on security behaviour intention, which has made this factor of high importance in its inclusion in the framework. Nevertheless, there is a possibility that when employees in Nigerian banks are aware that their activities are being monitored, and are possibly caught, the employees will take the proactive action to comply with ISSsPs. In the Nigerian banking sector, deterrence mechanisms like certainty of detection are more useful in developing the framework for promoting ISSsPs.

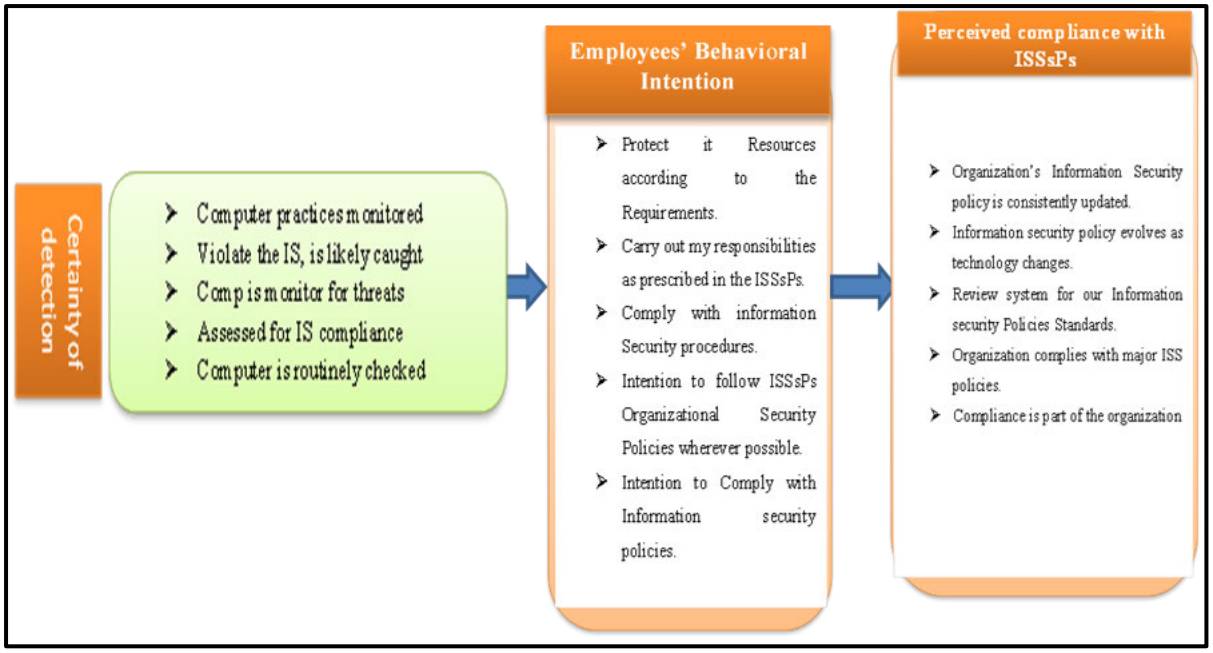


Figure 7.3: Certainty of Detection Influencing ISSsPs (Source: Author's Own)

7.3.4 Effectiveness of ISSsPs

Effectiveness of ISSsPs is a major factor in proffering solutions to information security breaches in Nigeria. This is in agreement with the study of Cheng *et al*. (2013). However, shown in Figure 7.4 is the influence of the perceived effectiveness of ISSsPs on the ISSsPs. The result of the analysis found all the included items significant. The banking industry in Nigeria will comply with ISSsPs if the effectiveness of the ISSsPs is assured, that is, when the employees have the perception of the standards and the policies. In addition, the hypothesis stated in Section 3.7 conforms to the ability of the perceived effectiveness of ISSsPs in influencing intention to comply with ISSsPs. Moreover, the six items subjected to factor analysis were found significantly important, which were later incorporated into the framework.

The effectiveness of the ISSsPs is the key to the organisation's information security compliance, and if there is compliance amongst the employees and the effect is positive, this will motivate employees to further adhere to ISSsPs in order to reduce insider threats. In relation to the finding of Wu *et al*. (2020), who declared that fair enforcement of ISP affects the increase in information security effectiveness, this factor is worth inclusion in the development of the framework.

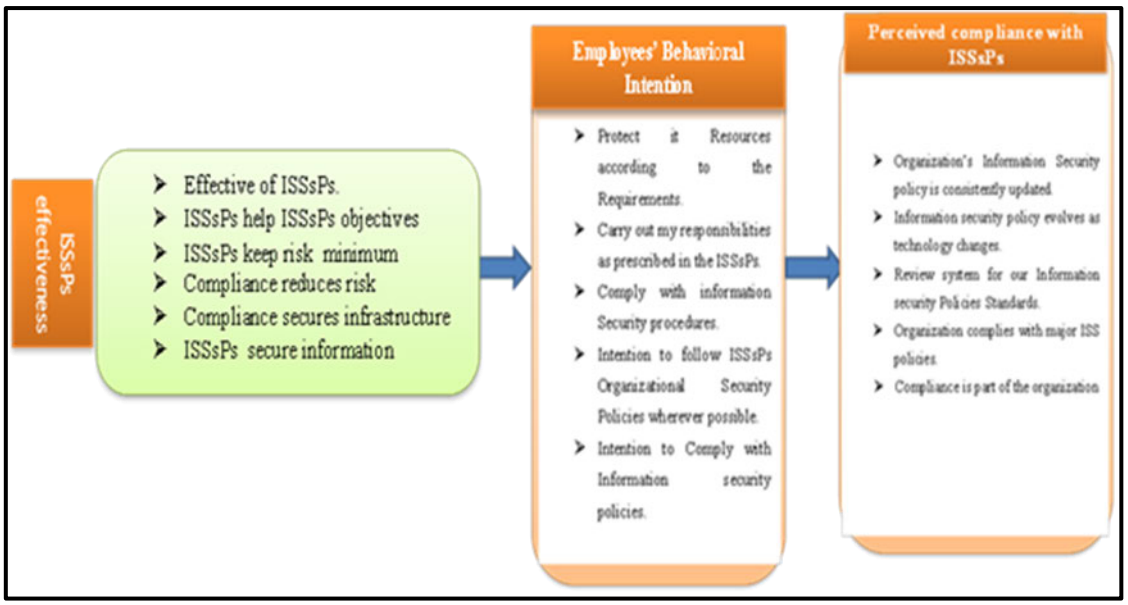


Figure 7.4: ISSsPs Effectiveness Influencing ISSsPs (Source: Author's Own)

7.3.5 Awareness of Information Security Threats

This motivational factor (awareness of information security threats) measured the extent of employees' awareness of information security threats through self-education, organisational programmes and on-the-job training, as indicated by Gundu and Flowerday (2013). Table 4.5 presented the seven initial items of awareness of information security threats, which were later reduced to four items after carrying out the EFA. The items include: IS threats communicated, IS training included, ISSsPs are discussed and updates me on ISSsPs changes.

Awareness of information security threats has been found significant by Gundu and Flowerday (2013) to be a factor that influences compliance with ISSsPs positively, hence it has also been included in many other frameworks. It is a vital construct and its inclusion will increase the efficacy and efficiency of the framework. Summarily, employees' awareness of security threats will likely increase their compliance with ISSsPs. Figure 7.5 presents the awareness items and the influence of the intention to comply with ISSsPs.

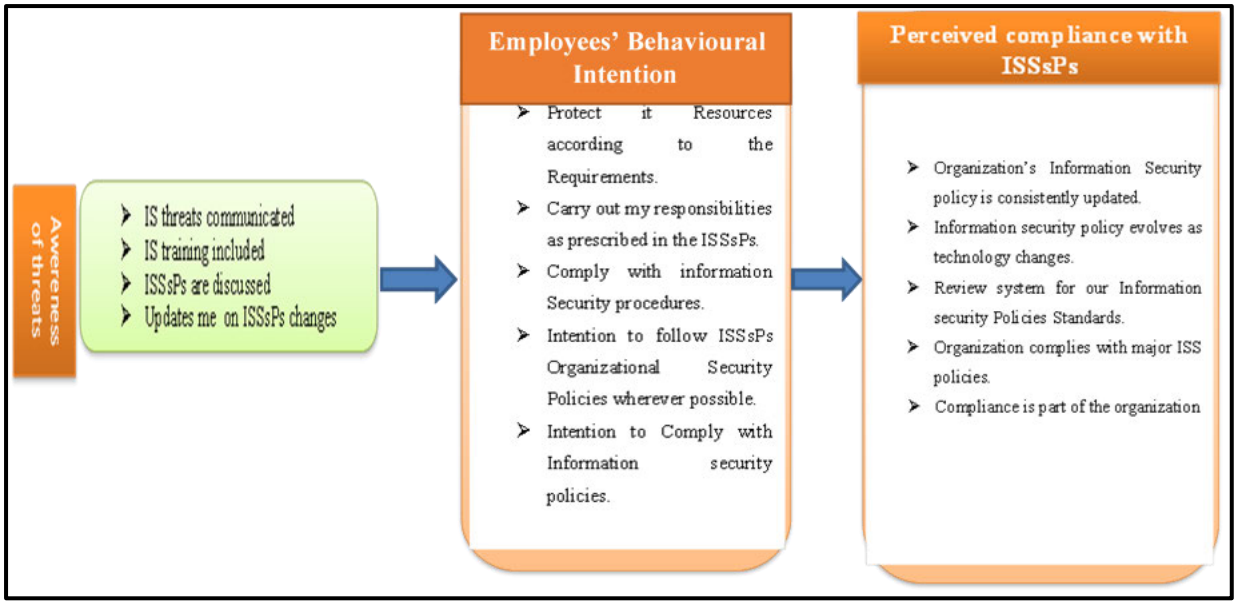


Figure 7.5: Awareness of InfSec Threats Influencing ISSsPs (Source: Author's Own)

7.3.6 Perception Bias

The results of this study consider perception bias as one of the predictors of ISSsPs compliance and the result implied a significant influence on ISSsPs. Eight items were presented for perception bias but after EFA, two items were found to be significantly important, which includes counteract InfSec threats and the mechanism in place. This is seen in Figure 7.6 and was confirmed in the study conducted by Williams *et al*. (2019), which found that perception bias significantly influences ISSsPs compliance amongst employees in the banking sector.

According to the theory of planned behaviour, optimism bias measures empirically by comparing the person's perception before an event takes place with the outcomes that transpire. Therefore, employees in Nigerian banks will likely be biased in making choice either to comply or not depending on their judgement. In predicting intention to comply, the study found that perception bias plays an important role by significantly influencing intention to comply with ISSsPs. Consequently, the framework embraces the inclusion of the construct. It is therefore suggested that compliance with ISSsPs should be enforced by management or by the superior personnel in the banking sector.

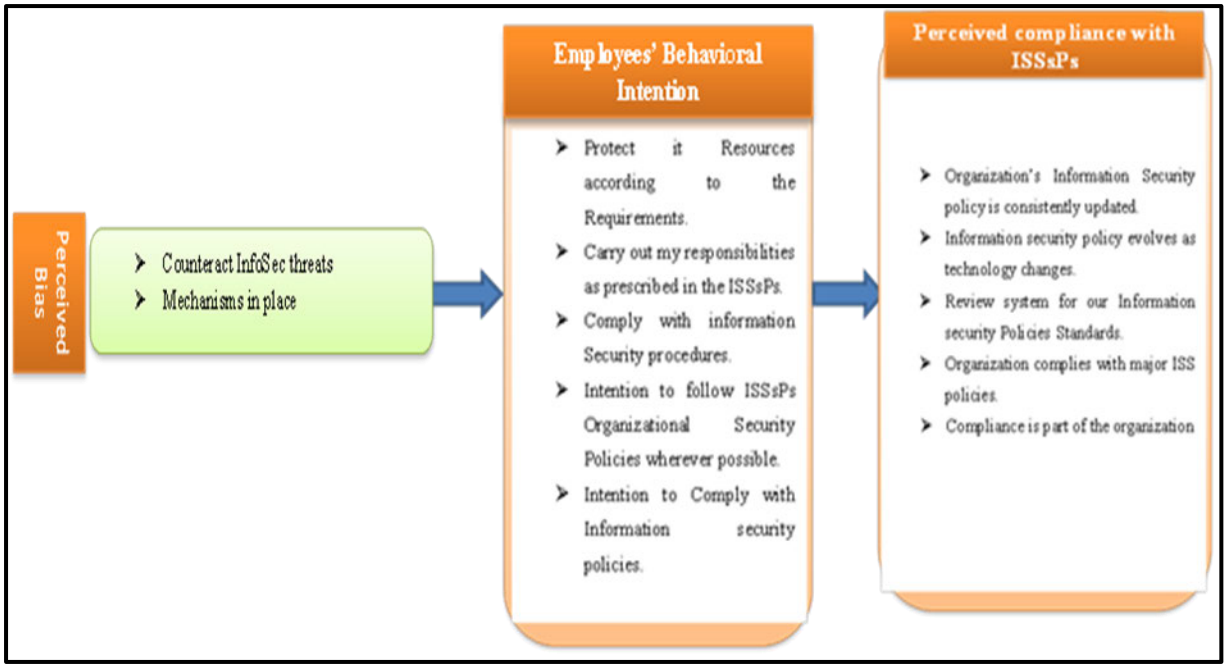


Figure 7.6: Perception Bias Influencing ISSsPs (Source: Author's Own)

7.3.7 Employees Intention to Comply and Actual Compliance with ISSsPs

It is important to show the relationship between the intention to comply with the actual compliance. Many researchers and studies have been conducted using employees' behavioural intention to predict the behaviour change of employees in terms of security policies compliance, which is in agreement with the conclusion of Siponen *et al*. (2014). This has proven that employees' behavioural intention to comply influences information security policies.

This study investigated intention to comply with ISSsPs through the lens of three theories, namely self-efficacy, the theory of planned behaviour and protection motivation theory. The initial items assigned for the employees' behavioural intention were six. The EFA in Tables 7.1 and 7.2 show the significant items, as one of the items was dropped, leaving five for the framework development. The items are:

- Protect IT resources according to the requirements.
- Carry out my responsibilities as prescribed in the ISSsPs.
- Comply with information security procedures.
- Intention to follow ISSsPs organisational security policies wherever possible.
- Intention to comply with information security policies.

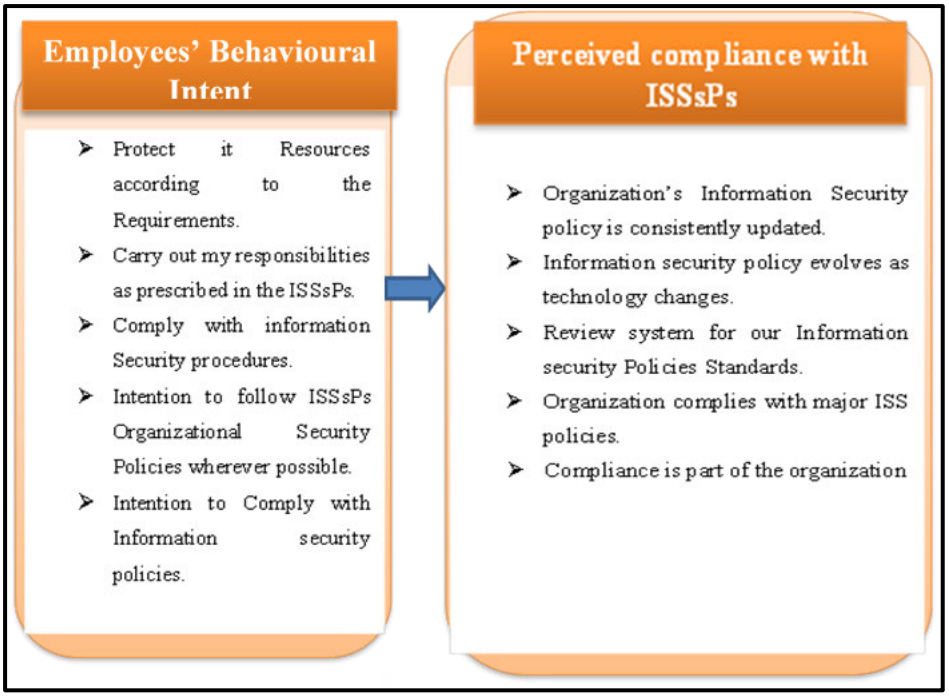


Figure 7.7: Employees' Behavioural Intention Influencing ISSsPs
(Source: Author's Own)

7.4 Employees' Compliance Framework

The individual factors influencing ISSsPs compliance have been considered important in mitigating insider threats amongst employees. However, Sections 7.3.1 to 7.3.7 show how individual motivational factors influence the intention to comply with the actual compliance before combining all the factors. In this section, all the significant motivational factor items were put together to form the framework. Shown in Figure 7.8 is the presentation of the framework. Hence, the components of the model are shown in Table 7.1, which are the significant items after carrying out the exploratory factor analysis. These provided answers to the fourth research question, which resulted in the development of the employees' compliance framework. There are six motivational factors, namely normative belief, information security threats awareness, perceived bias, perceived effectiveness of ISSsPs, certainty of detection and severity of penalty. The arrow connecting the motivational factors with the intention to comply in Figure 7.8 shows how the individual motivational factors influence intention to comply with international information security standards and policies in the banking sector. The retained items of each motivational factor are contained in each of the factors after EFA was conducted. Intention to comply is another construct in the model. Consequently, this construct contained five significant items after EFA has been conducted.

Table 7.1: Components of ISSsPs Compliance Framework

Constructs name	Description of Construct item
Information Security Standards and policies Compliance	Organisation's Information Security policy is consistently updated
	Information security policy evolves as technology changes.
	Review system for our Information Security Policies Standards.
	Organisation complies with major ISS policies.
	Compliance is part of the organisation
Normative Belief	Co-worker sees me as ethical
	I should comply with ISSsPs.
	Assesses my work
	It is important to comply
Information Security threats Awareness	IS threats communicated
	IS training included
	ISSsPs are discussed
	Updates me on ISSsPs changes
Perceived Effectiveness of ISSsPs	Effective of ISSsPs.
	ISSsPs help ISSsPs objectives
	ISSsPs keep risk minimum
	Compliance reduces risk
	Compliance secures infrastructure
	ISSsPs secure information
Perceived Bias	Counteract InfoSec threats
	Mechanisms in place
Certainty of Detection	Computer practices monitored
	Violate the IS, is likely caught
	Comp is monitor for threats
	Assessed for IS compliance
	Computer is routinely checked
Severity of Penalty	Punishing employees that break IS
	Breaker of IS can rules lose their jobs
	Violating ITSEC severely punished.
Employees Behavioural Intention	Protect it Resources according to the Requirements.
	Carry out my responsibilities as prescribed in the ISSsPs.
	Comply with information Security procedures.
	Intention to follow ISSsPs Organisational Security Policies wherever possible
	Intention to Comply with Information security policies.

The item represents behavioral intention to carry out information security standards and policies compliance practices. There is a link between intentions to comply and the actual compliance (ISSsPs). The arrow represents how the behavioral intention influences the ISSsPs.

Furthermore, the actual compliance (ISSsPs) contains the remaining five significant items after EFA. This construct housed the actual practice of the information security standards and policies in the banking sector. All the components are assembled together to present the employees' compliance framework in the Nigerian banking sector. Importantly, motivational factors are employed to promote information security standards and policies compliance. When these factors are dutifully followed, insider threats will be curtailed, with an attendant reduction in cybercrime.

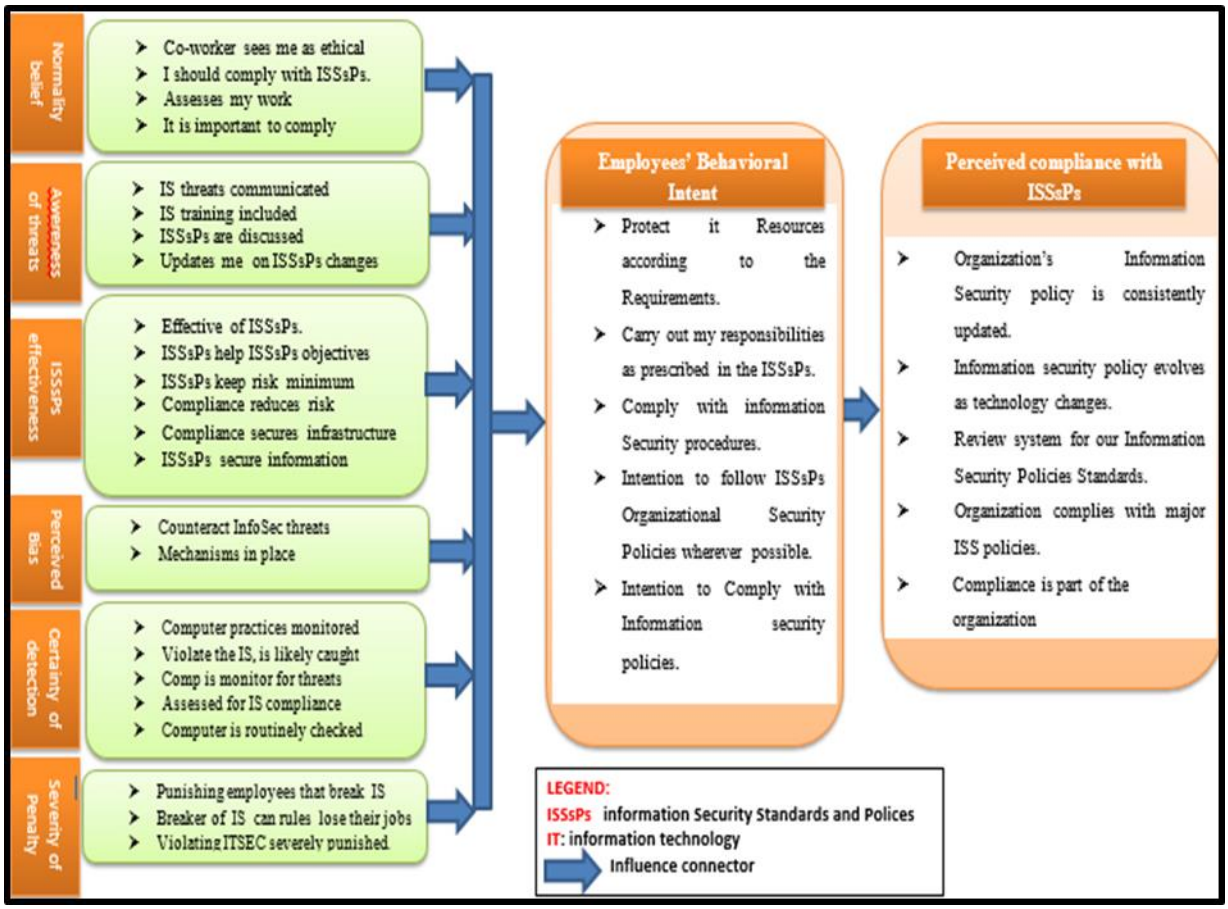


Figure 7.8: Employees' Information Security Standards and Policies Compliance Framework (Source: Author's Own)

7.5 Framework Validation

Evidence whether a particular system meets its security requirements is validated, which provides confidence that a system satisfies stated objectives (Ofusori, 2019). Hence, to validate that an ISSsPs compliance framework for banking institution in Nigeria meets the information security standards and policies compliance functionality, the unified and collective opinions of the participating banks' employees (particularly executives, heads of operations, ICT

department personnel and executive managers) are sought. It is however necessary to validate the framework in order to ensure the generality and the effective functionality of the implementation of the framework. The validation results are discussed in Section 7.6.

7.6 Criteria for Selecting the Validation Expert

In selecting experts for the validation of the proposed ISSsPs compliance framework, the fact that information security is not new in the banking sector in Nigeria means that there is therefore no challenge in the selection of the experts in the validation process. These experts were purposively selected looking at their track records in the industry as bankers. They were selected based on the following criteria:

1. Having extensive working experience in the banking sector and knowledge of information security.
2. Having in-depth knowledge and expertise of the concepts of information security.
3. Having recent hands-on experience in policies and standards in relation to information security.
4. Having extensive involvement in information security management.

Moreover, serious concern was given to the willingness of the experts to participate in the validation exercise. Furthermore, to maintain inclusiveness due to the nature of this research and to maintain heterogeneity, a deliberate effort was made to ensure appropriate representation.

7.7 Background Information on the Validation Team Members

Tables 7.2 to 7.5 show the area of specialisation, experience, level of familiarity with information security and level of involvement of the validation experts in information security standards and policies. The demographic (background) information of the team of experts selected for the validation of the proposed framework is depicted in Tables 7.2 to 7.5. Descriptively, the areas of specialisation are: Head of operations (14.3%), System maintenance officer (14.3%), Human resource manager (7.1%), Quality controller (21.4%) and others (42.9%). For the years of experience, 10-15 years (57.1%, 16-20 years (35.7%) and 21-25 years (7.1%) were shown. In relation to familiarity of the experts with ISSsPs, 14.3% of them indicated somehow familiar; 28.6% are familiar, while 57.1% are very familiar. Moreover, as per their involvement in ISSsPs, less than 25% (14.3%), between 25 and 50% (21.4%), 51-

75% (42.9%) and above 75% (21.4%) was indicated. Therefore, in reference to the background information of the respondents, it shows that they are well experienced experts in information security.

Table 7.2: Area of Specialisation

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Head of Operations	2	14.3	14.3	14.3
	System Maintenance Officer	2	14.3	14.3	28.6
	Human Resource Manager	1	7.1	7.1	35.7
	Quality Controller	3	21.4	21.4	57.1
	Others	6	42.9	42.9	100.0
	Total	14	100.0	100.0	

Table 7.3: Years of Experience

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	10-15 years	8	57.1	57.1	57.1
	16-20 years	5	35.7	35.7	92.9
	21-25 years	1	7.1	7.1	100.0
	Total	14	100.0	100.0	

Table 7.4: Familiarity with ISSsPs

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Somehow familiar	2	14.3	14.3	14.3
	Familiar	4	28.6	28.6	42.9
	Very familiar	8	57.1	57.1	100.0
	Total	14	100.0	100.0	

Table 7.5: Involvement in ISSsPs

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Less than 25%	2	14.3	14.3	14.3
	25-50%	3	21.4	21.4	35.7
	51-75%	6	42.9	42.9	78.6
	Above 75%	3	21.4	21.4	100.0
	Total	14	100.0	100.0	

7.8 Data Analysis of Experts' Ratings

Five dimensions are the focus of the proposed framework in relation to its validation, namely: appropriateness of the framework for information security compliance; adequacy in addressing all the identified information security issues; feasibility in relation to cost-saving; timing and resources, flexibility in the usage of the framework; as well as intention to use by the bankers.

7.9 Descriptive Analysis of the Validation Questionnaire

A descriptive analysis was conducted on the different aspects of the compliance framework. The results of the analysis are presented in Table 7.6, as well as Sections 7.9.1 to 7.9.6.

Table 7.6: Attributes of the Framework

Description of the Attributes	Scores/Mean Score						
	6	**5**	**4**	**3**	**2**	**1**	**Mean Score**
Appropriateness							
In line with the policies and strategies of the bank	4	2	4	4	0	0	4.43
Enhances the effectiveness of the information security standards	4	2	4	4	0	0	4.43
Contribution to compliance of employees	3	4	3	4	0	0	4.43
Adequacy							
Addressing identified information security issues	2	4	2	6	0	0	4.14
Reduction of information security breaches	4	1	5	4	0	0	4.36
Feasibility							
Can be cost-effective	2	6	1	5	0	0	4.36
Can be implemented within a short period of time	3	2	5	3	0	1	4.14
Can be implemented with the available resources of the bank.	3	5	0	6	0	0	4.36
Flexibility							
Can be easily adopted with changing policies.	3	3	4	4	0	0	4.36
Can be adopted for mitigating information security threats within different branches of the bank.	5	4	2	3	0	0	4.07

7.9.1 Appropriateness

7.9.1.1 Employees' Compliance Framework in Line with the Policies and Strategies of the Bank

Regarding *question number one* on appropriateness, the experts were to indicate their opinions on whether the framework is in line with the policies and strategies of the bank. The result of the assessment is illustrated in Figures 7.9 to 7.10. Figure.7.9 reports that 25 % of the participants strongly agreed, while 25 % agreed and 25% slightly agreed that the employees' compliance framework aligned with the policies and strategies of the bank. Moreover, 25% of the experts responded to slightly disagree. The submission of the outcome of the analysis has found that the vast majority of participants believed that the ISSsPs is in line with the policies of the banks. According to Ofusori (2019), policies are formed by uniting the different opinions of top managers.

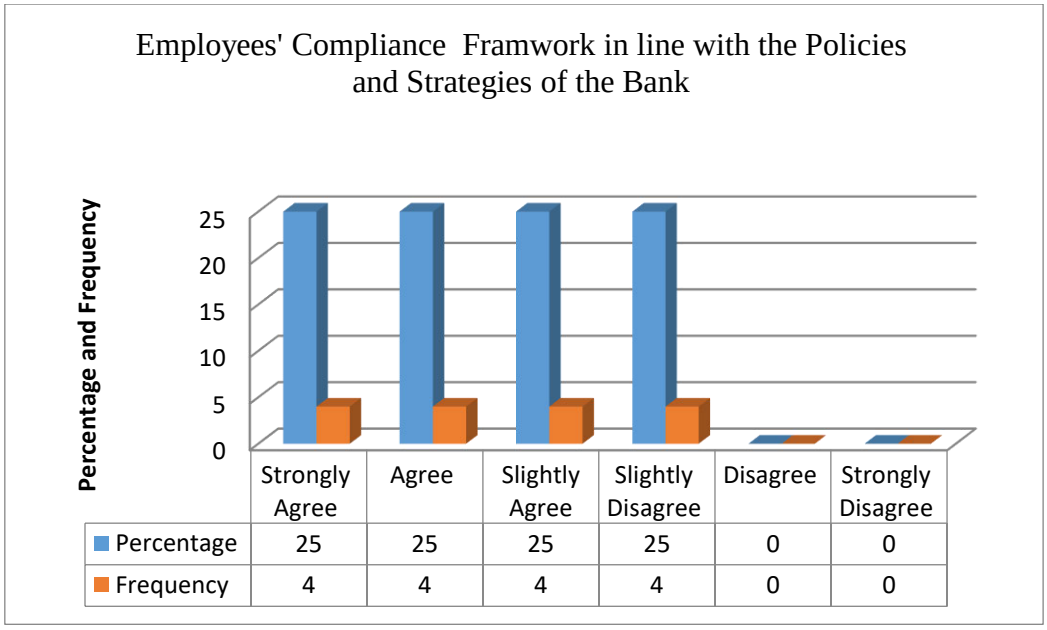


Figure 7.9: Employees' Compliance Framework in Line with the Policies and Strategies of the Bank

7.8.1.2 Employees' Compliance Framework Enhances the Effectiveness of the Information Security Standards

The outcome in Figure 7.10 indicates that 28% of the experts strongly agreed with the statement, 14.3% agreed and 28% slightly agreed, while only 28% slightly disagreed with the statement. 70.3% of the experts collectively agreed that the security framework enhances the effectiveness of the bank's information security. This indicates that the employees' compliance framework enhances the effectiveness of the information security standards and policies of the banks, in congruence with Cameron and Whetten (2013). The implementation of the employees' compliance framework aims at achieving the success factors for information security standards and policies compliance within Nigerian banks.

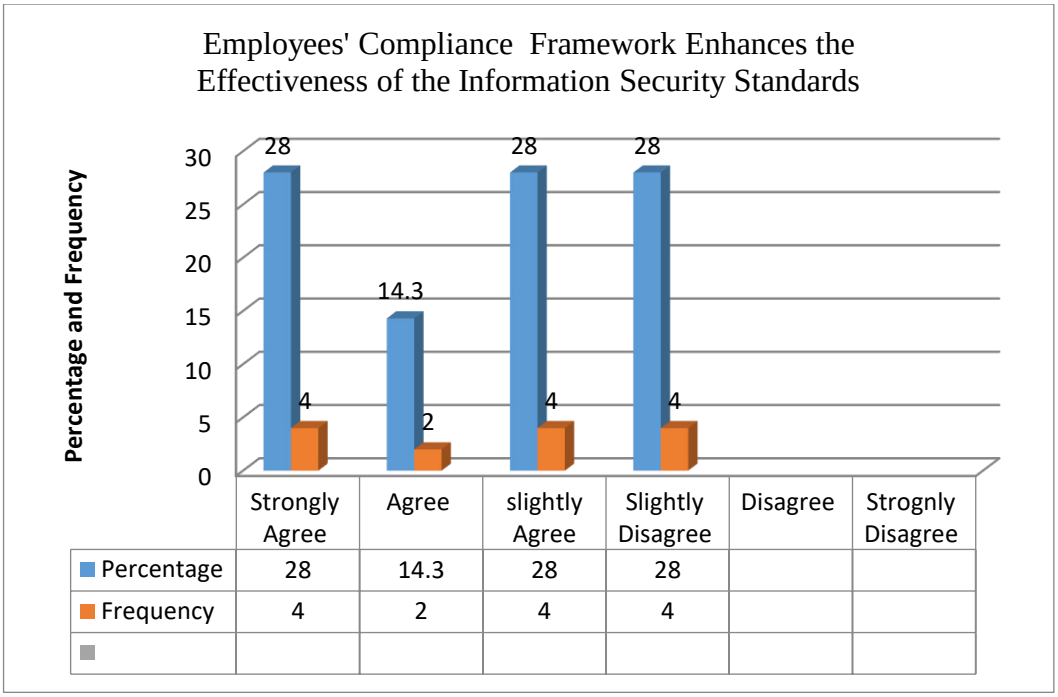


Figure 7.10: Employees' Compliance Framework Enhances the Effectiveness of the Information Security Standards

7.8.1.3 Framework's Contribution to Compliance of Employees

Figure 7.11 shows the responses of the experts regarding the contribution of the framework to their organisation. Consequently, 21.4% strongly agreed that the employees' compliance framework should contribute to the bank's operational efficiency, 28.6% agreed, while 21.4% slightly agreed.

In addition, 28.6% slightly disagreed with the statement. The outcome of the analysis indicates that most participants (71.4%) submitted that the employees' compliance framework developed for Nigerian banks can contribute to the efficiency of the banks' development in in terms of operation and information security issues. Kamatchi and Modi (2016) asserted that the efficiency of an information security framework depends on its ability to be utilized with little maintenance. In the same vein, the information security framework is said to be efficient if it has the ability to detect and reduce information security threats, according to Ofusori (2019).

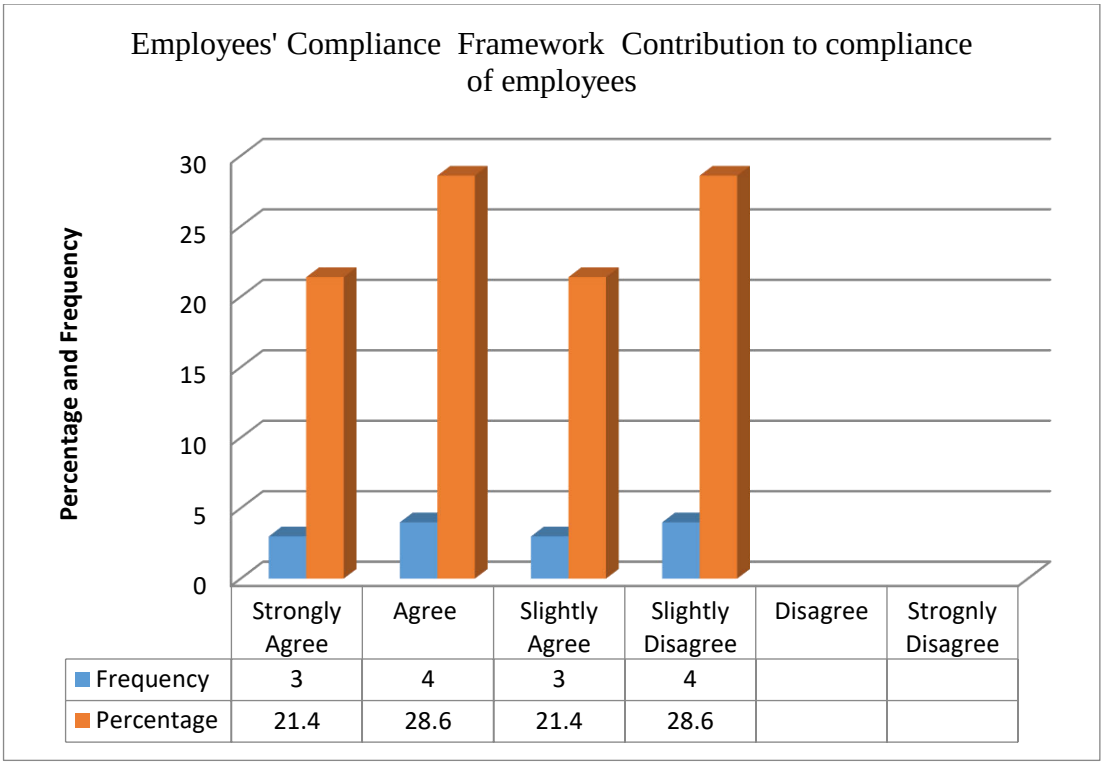


Figure 7.11: Employees' Compliance Framework Contribution to Compliance of Employees

7.9.2 Adequacy

In reference to *question number two*, it requested feedback on the adequacy of the framework to address all the identified information security issues pertaining to compliance.

7.9.2.1 Employees' Compliance Framework Addressing Identified Information Security Issues

Experts assessed the criteria presented in item 2 of the validation questions (Appendix F) to determine whether the employees' compliance framework was adequate. The assessment is illustrated in Figures 7.12 and 7.13 . In Figure 7.12, it is indicated that 14.3% of the participants strongly agreed, 28.5% agreed, while 14.3% slightly agreed that the employees' compliance framework could address all the information security standards and policies. Additionally, 42.9% slightly disagreed with this statement. It shows that a greater portion of the participants (57.1%) agreed that the framework addresses any information security issues by reducing information security breaches. This shows that compliance with information security standards and policies reduces information security breaches and cybercrime. According to Cox (2012), employees will be more conscious of the need to comply with security standards if they have a clearer understanding of ISSsPs and the consequences of information security breaches. Koohang *et al*. (2020). The experts that slightly disagreed with the statement that the

employees' compliance framework can address identified information security issues based their opinions on the belief that the adoption of IT tools for combatting information security breaches is more effective than employing human factors. Moreover, using the human factor is more effective when it comes to combatting insider threats in reducing cybersecurity.

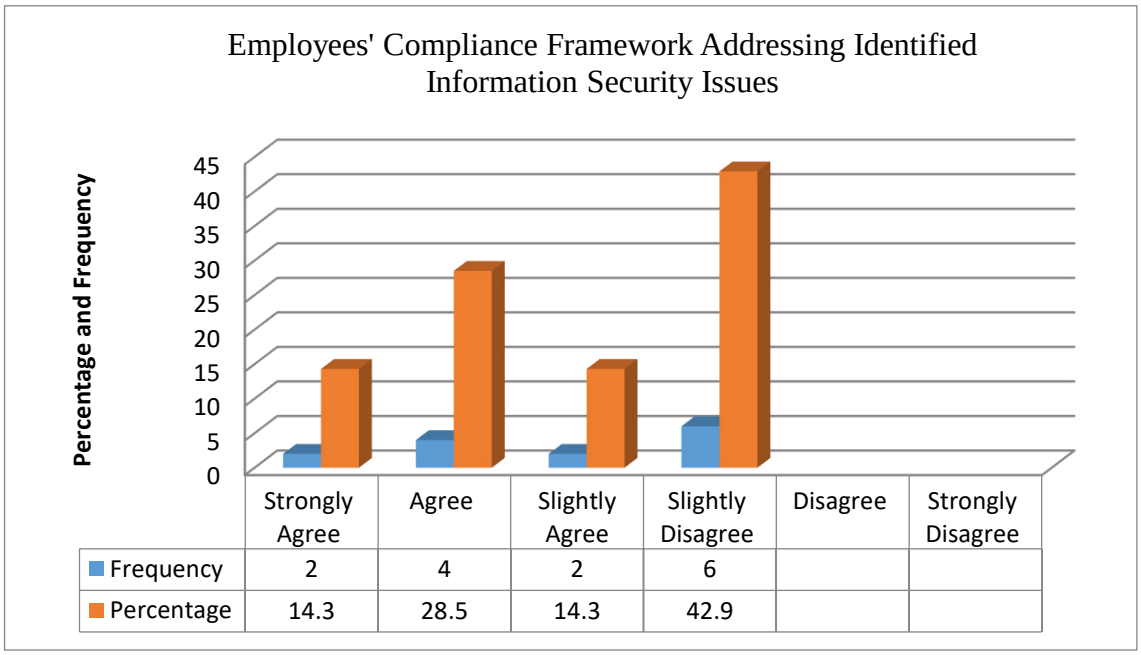


Figure 7.12: Employees' Compliance Framework Addressing Identified Information Security Issues

7.8.2.3 Employees' Compliance Framework Reduces Information Security Breaches

Figure 7.13 indicates that 25% of the experts strongly agreed, while 6.2% agreed and 31.3% slightly agreed. A significant portion of the participants (62.5%) believed that the employees' compliance framework could address all the social threats identified. The remaining participants slightly disagreed with this statement. The outcome of the analysis shows that a majority of the participants affirmed that ISSsPs reduces information security breaches when it is dutifully followed, while information security breaches arise from employees who are careless with the information security of the organisation. Following the result in objective two, there are still information security breaches yet to be averted. Hence, this framework should be considered as a tool that may assist the organisation in combatting insider threats.

Summarily, reference is made to Bello *et al*. (2015), who believe that organisations should be cognizant of the negative consequences of a security breach and address them accordingly.

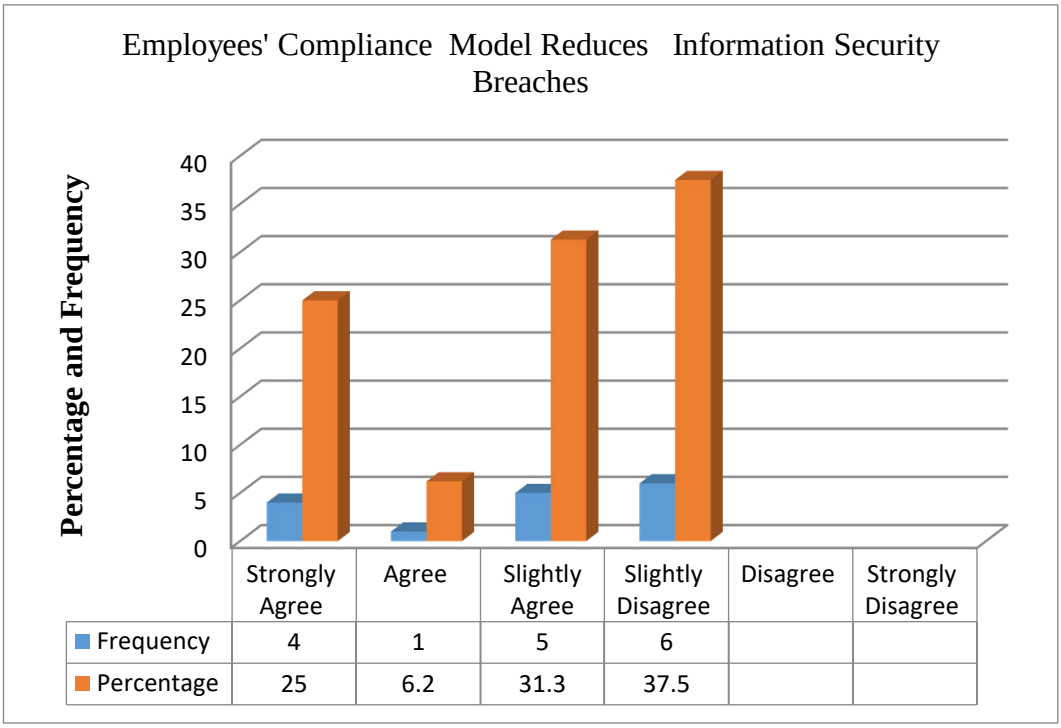


Figure 7.13: ISSsPs Framework Reduces of Information Security Breaches

7.9.3 Feasibility

Respondents assessed the framework based on their experience. Figures 7.6 to 7.8 contain the responses on the feasibility of the framework.

7.9.3.1 Cost-Effectiveness of the Framework

Figure 7.14 presents the responses of the experts regarding the cost-effectiveness of the implementation of the framework. It was shown that14.3% of the experts strongly agreed, 42.9% agreed, while 7.1% slightly agreed that the employees' compliance framework is cost-effective. Furthermore, 35.7% slightly disagreed with the statement. 64.3% affirmed that the employees' compliance framework could be implemented in the organisation with little cost. This is in conformity with Asheri *et al*. (2012), who declared that the parameters used in measuring the performance of information system are budgets; performance; cost and return on investment, and its fitness for purpose (Su, 2016). With the submission of the respondents, this clearly shows that the implementation of the employees' compliance framework could be done with little or no cost.

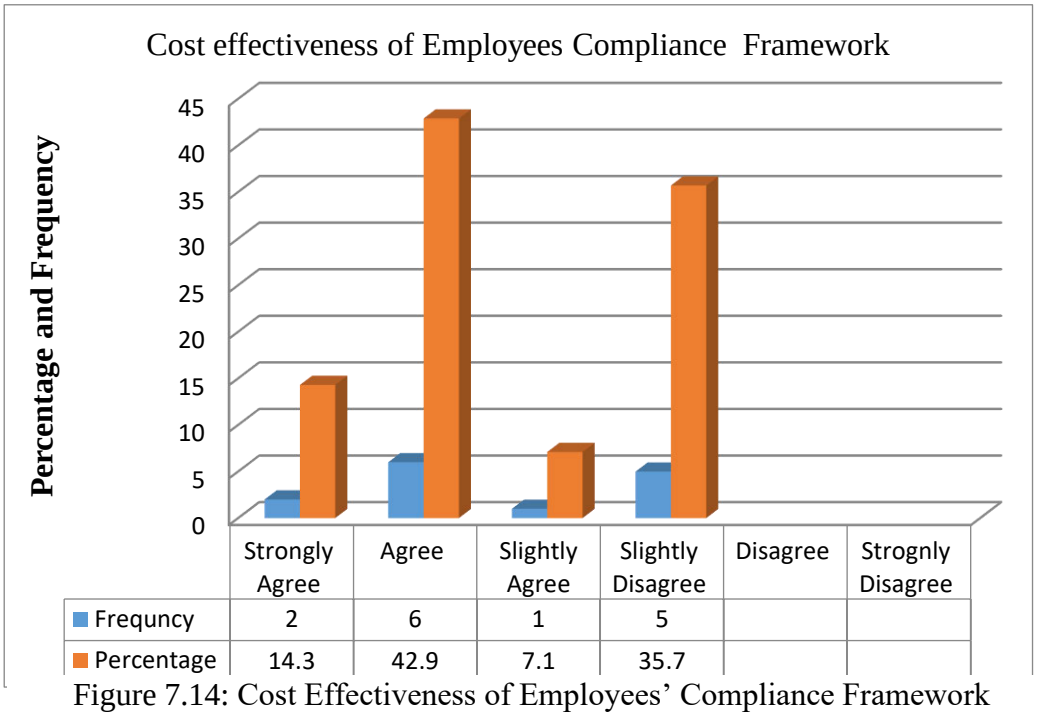


Figure 7.14: Cost Effectiveness of Employees' Compliance Framework

7.8.3.2 Can be implemented within a Short Period of Time

The result in Figure 7.15 shows that 23.1% of the study participants strongly agreed, 15.3% agreed, 38.5% slightly agreed, while 23.1% slightly disagreed that the employees' compliance framework could be implemented within a short period of time. This informs the researcher that a majority (76.9%) of the experts indicate that the employees' compliance framework could be implemented within stipulated time in Nigeria's banking sector. Furthermore, this indicates that the organisation has available infrastructure to implement the employees' compliance framework within a given time and period. This is in line with the declaration of Cameron and Whetten (2013), which acknowledged that timeline feasibility is very crucial in examining whether the organisation has the capability of implementing the employees' compliance framework within a specified period. Furthermore, Hong (2013) stated that there is need for an organisation to have the required resources and capabilities to implement the framework within a short time-frame.

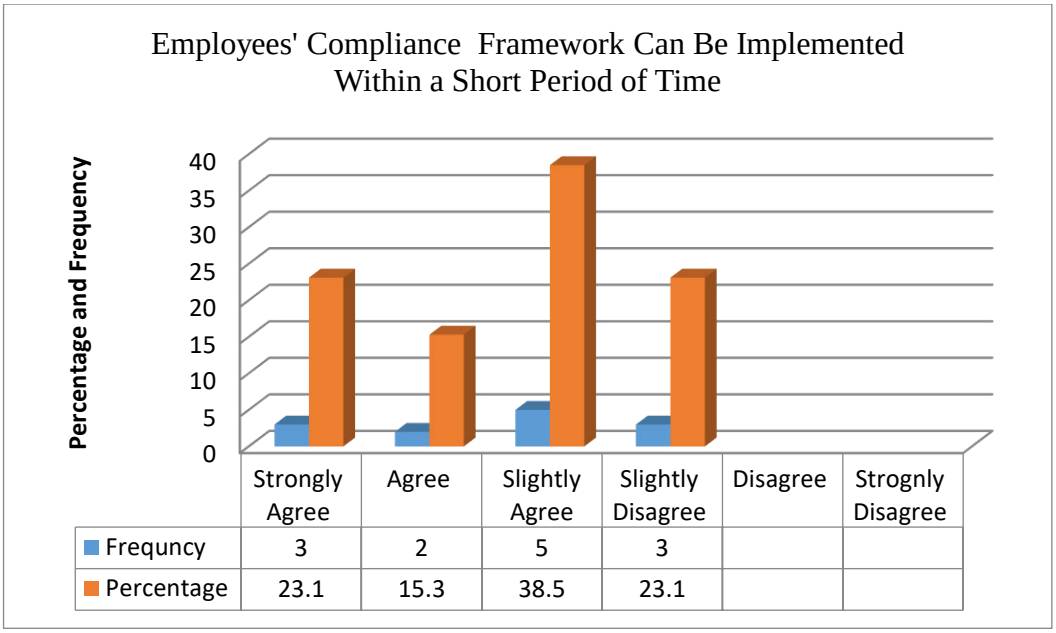


Figure 7.15: ISSsPs Framework can be Implemented within a Short Period of Time

7.8.3.3 Employees' Compliance Framework can be Implemented with the available Resources of the Bank

Figure 7.16 shows the responses of the experts that agreed and disagreed with the statement of "employees' compliance framework can be implemented with the available resources of the bank". Consequently, 21.4% strongly agreed, while 35.7% agreed, bringing it to a total of 57.1%, indicating that implementation of the framework can be done with the available resources of the bank. Furthermore, 42.9% slightly disagreed with the statement. This indicates that a majority of the participants agreed with the statement that the employees' compliance framework can be implemented with the available resources of the bank. This is in agreement with the assertion of Ofusori (2019) that the feasibility of implementing an employee compliance framework absolutely depends on the available resources of the organisation and the ability to give support to the process of implementation. In addition, 42.9% of the participants of the study did not believe that the employees' compliance framework can be implemented with the available resources in Nigerian banks. With the greater percentage agreeing to the fact that it can be implemented with the available resources in the bank, the implementation process will be carried out un-resisted.

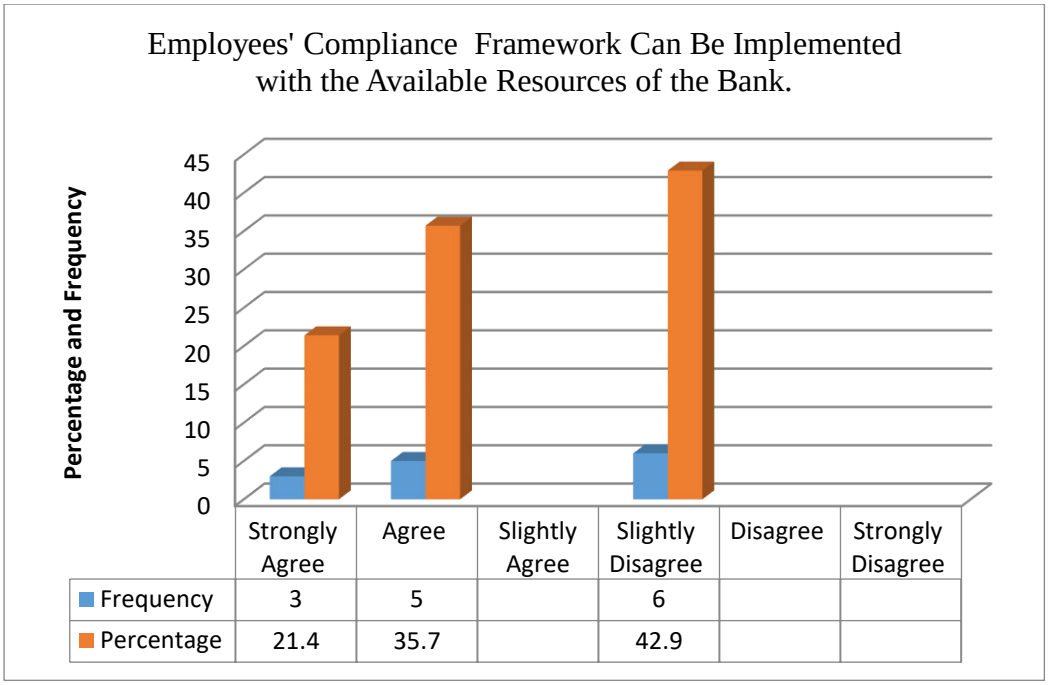


Figure 7.16: Employees' Compliance Framework can be Implemented with the Available Resources of the Bank

7.9.4 Flexibility

The experts were requested to give their opinion on the criteria presented in Item 4 of the validation questions (Appendix F) in order to examine the flexibility of the employees' compliance model. The result of the analysis can be seen in Figures 7.17 and 7.18. In Figure 7.9, 21.4% strongly agreed, 21.4 % agreed with the statement, while 28.6% slightly agreed that the framework can be adopted without difficulty, in spite of changing policies. Contrarily, 28.6% slightly disagreed with the option. The outcome of the analysis indicates that a greater portion of participants (71.4%) confirmed that the employees' compliance framework could be easily adopted in spite of changing policies, which according to Ifinedo (2012), is crucial. According to Cerna (2013), policy change occurs when there is an interaction between external changes and the success of the ideas. Moreover, 28.6% of the participants somewhat disagreed that the employees' compliance framework can be adopted with changing policies. This is as a result of a lack of consistency and quick response in adopting standards and review of the standards across the banking sector, as discovered with the issues of ISO/IECISO/IEC 27001. Hence, as standards and policies guidelines change, it is required by the bank to flow with the trend to secure banks' information and assets, as the using of technology to fight insider threats cannot be enough, which is in corroboration with Peterson's (2014) work.

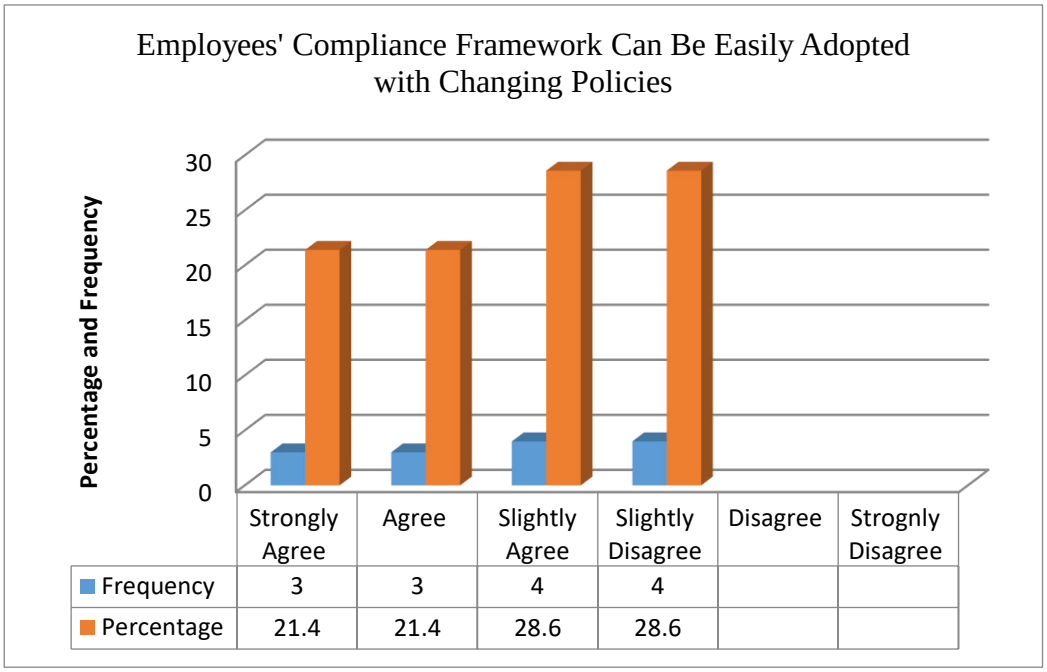


Figure 7.17: Employees' Compliance Framework Can Be Easily Adopted with Changing Policies

7.8.4.1 The Framework Can Be Adopted in Mitigating Information Security Threats within Different Branches of the Bank

In relation to the last question on flexibility, the question posits: "*Can it be adopted for mitigating information security threats within different branches of the bank?"* The result is shown in Figure 7.18. Indications are that 35.7% of the participants strongly agreed, 28.6% agreed and 14.3% slightly agreed that the employees' compliance framework can be adopted in mitigating security threats within different branches of the bank. Only 21.4% slightly disagreed with the statement. With the results of the analysis, and in relation to a greater proportion (78.6%) of the respondents agreeing with the adoption of the compliance framework, indications are that the framework can be implemented across the selected banks and their branches. This study supports the findings of Vateva-Gurova *et al*. (2014) that a corporate business must possess the ability to survive during tempestuous incidents and to drive out sudden hard blows. This means that there must be room for the implementation of the employees' compliance framework and its survival amongst the selected banks and across their branches.

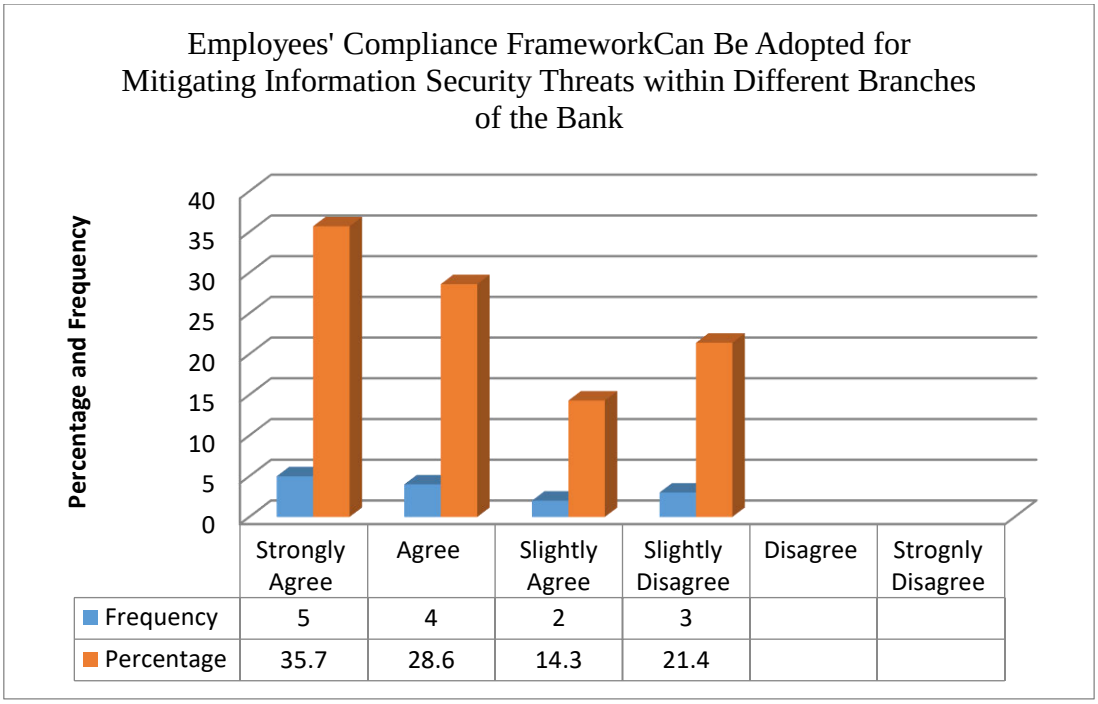


Figure 7.18: Employees' Compliance Framework Can Be Adopted for Mitigating Information Security Threats within Different Branches of the Bank

7.9.5 Intention to Use ISSsPs Framework

The experts were asked to assess the criteria presented in Item 5 of the validation questions (Appendix F) in order to determine the intention to use the framework. The outcome of the assessment is presented in Table **7.7.**

Table 7.7: Intention to Use

Intention to Use	**Yes**		**No**	
	f	**%**	**f**	**%**
Implementation of the framework without changes.	11	78.6	3	21.4
Readiness to adopt the framework immediately.	10	71.4	4	28.6
The usage of the framework by the employees will be easy.	14	100.0	0	0

7.8.5.1 Implementation of the Framework without Changes

Figure 7.19 reveals that 78.6% of the participants are in support of the implementation of the framework the way it is, without any changes. This affirms that participants are happy and comfortable with implementing the employees'compliance framework in their organisations.

The finding is in line with the study of Wolden *et al*. (2015), which found that the organisation is more comfortable with implementing a framework if the framework addresses the security issues of the organisation.

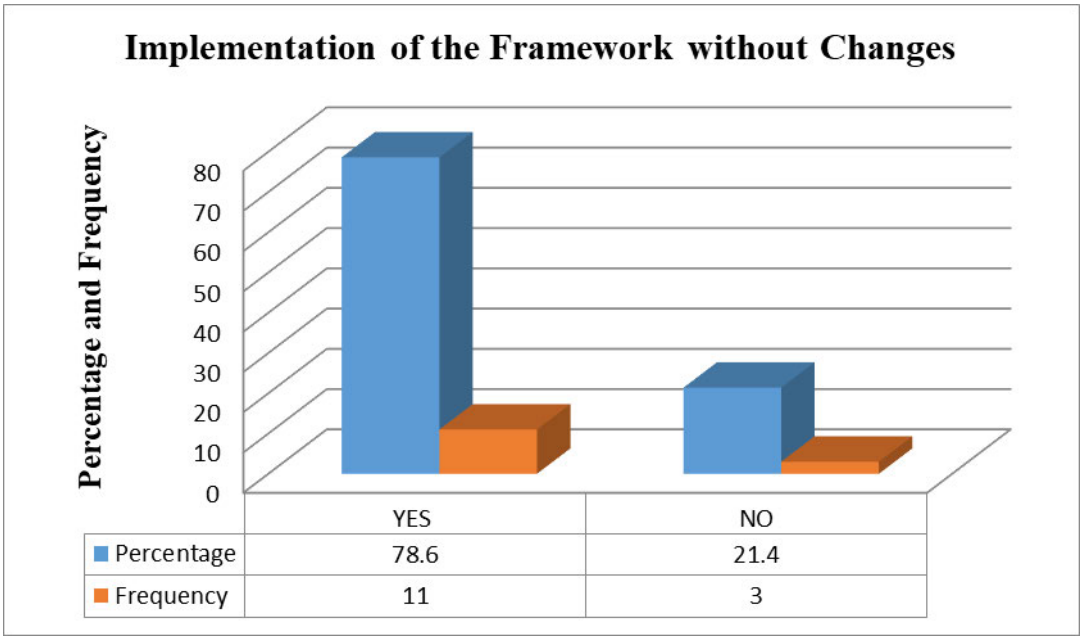


Figure 7.19: Implementation of the Framework without Changes

7.8.5.2 Readiness to Adopt the Framework Immediately

Figure 7.20 reveals that 71.4 % of the participants are willing to adopt the security framework immediately in their organisations. According to Cameron and Whetten (2013), organisations are more likely to adopt a security framework if it is flexible and efficient. However, 28.6 % of the experts who participated in the survey were of the opinion that adopting the framework should take place in the future. This may be arrogated to the financial constraints in the banks or failure to have budgets towards the implementation of the framework in the banking sector.

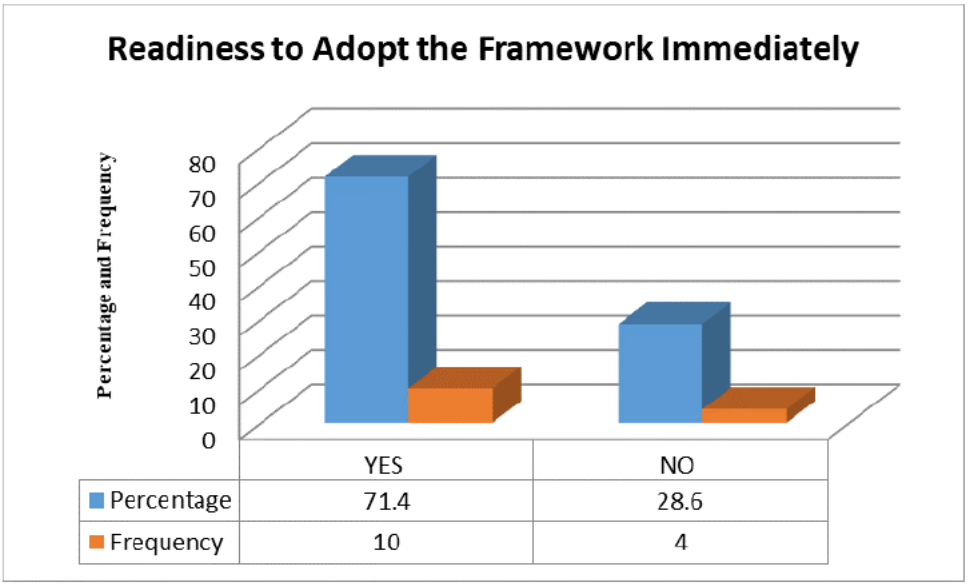


Figure 7.20: Readiness to Adopt the Framework Immediately

7.8.5.3 The Usage of the Framework by the Employees will be Easy

In relation to the acceptability of the usage of the framework and the analysis shown in Figure 7.21, it is seen that all the experts are in agreement (100%) on the easier usage of the employees' compliance framework. While Cameron (2014) declared that a framework is result-driven and it empowers versatility, Stouffer *et al.* (2008) submitted that it is this flexibility that enables the framework to be easily used by organisations.

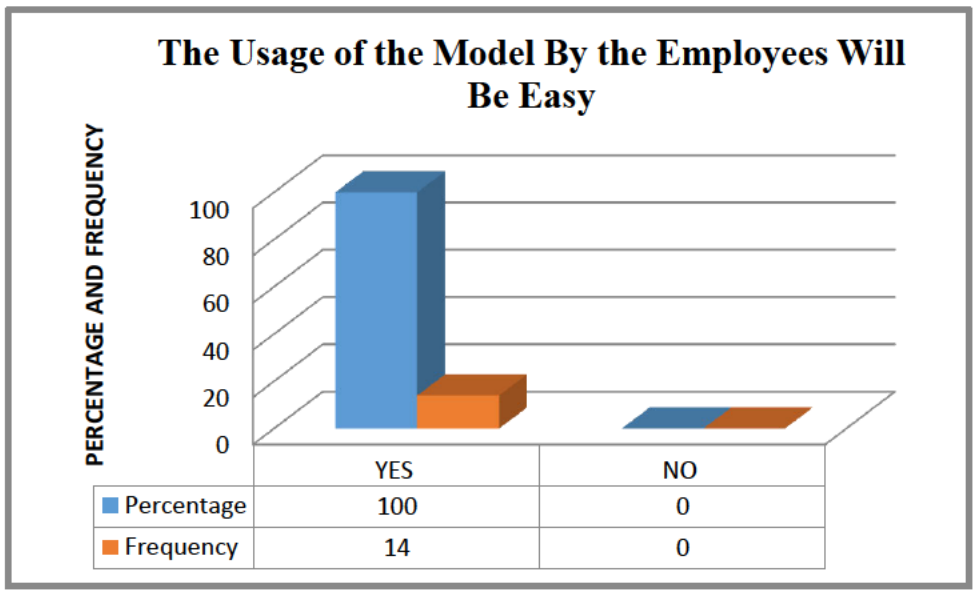


Figure 7.21: The Usage of the Framework by Employees Will Be Easy

7.9.6 Recommendation of the Experts

Section 6.4 of the questionnaire creates an avenue for the experts to make useful comments on the issues that were not discussed or included in the framework. Following this, three of the respondents indicated their intentions. The first expert stated that it is important to include continual commitment into the framework, while the second respondent indicated that the inclusion of regular training regarding international of ISSsPs compliance issues should be taken more serious and the third respondent opined that it is necessary to consider regular reviews of the framework content. The three respondents have given a profound contribution into the philosophical and theoretical aspects of the framework as the continual commitment, training and regular review of international information security standards and policies compliance are very important in enhancing employees' compliance with ISSsPs in the banking sector.

7.10 The Outcome of the Validation

Although individual characteristics of the validation have been done extensively in Sections 7.6 to 7.8, this chapter submit the empirical results of the analysis carried out to evaluate the employees'compliance framework (ISSsPs). The analysis result measure of acceptance of the framework wholly rests on characteristic such as appropriateness, adequacy, feasibility, flexibility and intention to use. The finding of the analysis was also supported by the literatures. It is important to note that the motivational factor sand how they have influenced employees' intention to comply with ISSsPs was taken into account step-by-step before the final full development of the framework. Furthermore, the framework was generally accepted for proactive intervention for motivating employees in complying with international information security standards and policies, with the intention to reduce insider threats which in turn reduces cybercrime in Nigerian banks. According to NIST (2014), an organisation will have interest in the implementation of a certain framework if such organisation knows that the framework can address the security issues of their organisation. From the finding in 7.12, the usage of the framework by employees will be easy, as the entire group of respondents (100%) indicated that the framework is easy to use. In terms of readiness to adopt the framework immediately, in Section 7.8.5.2 the majority of the respondent indicated that their banks are ready to adopt the framework immediately. Relating to information security issues, which is the main purpose of the framework, a significant number of respondents agreed that the framework can be used in mitigating information security threats within the banks. In Section 7.4, the three respondents made a useful suggestion to include certain elements such as

continual commitment, training and regular reviews. The elements are very important in adopting human behaviour to mitigate insider threats amongst the employees in the banking sector. Collectively, the outcome of the validation indicates the acceptability and credibility of the employees' compliance framework of ISSsPs. The framework is generally accepted in the banking sector for implementation.

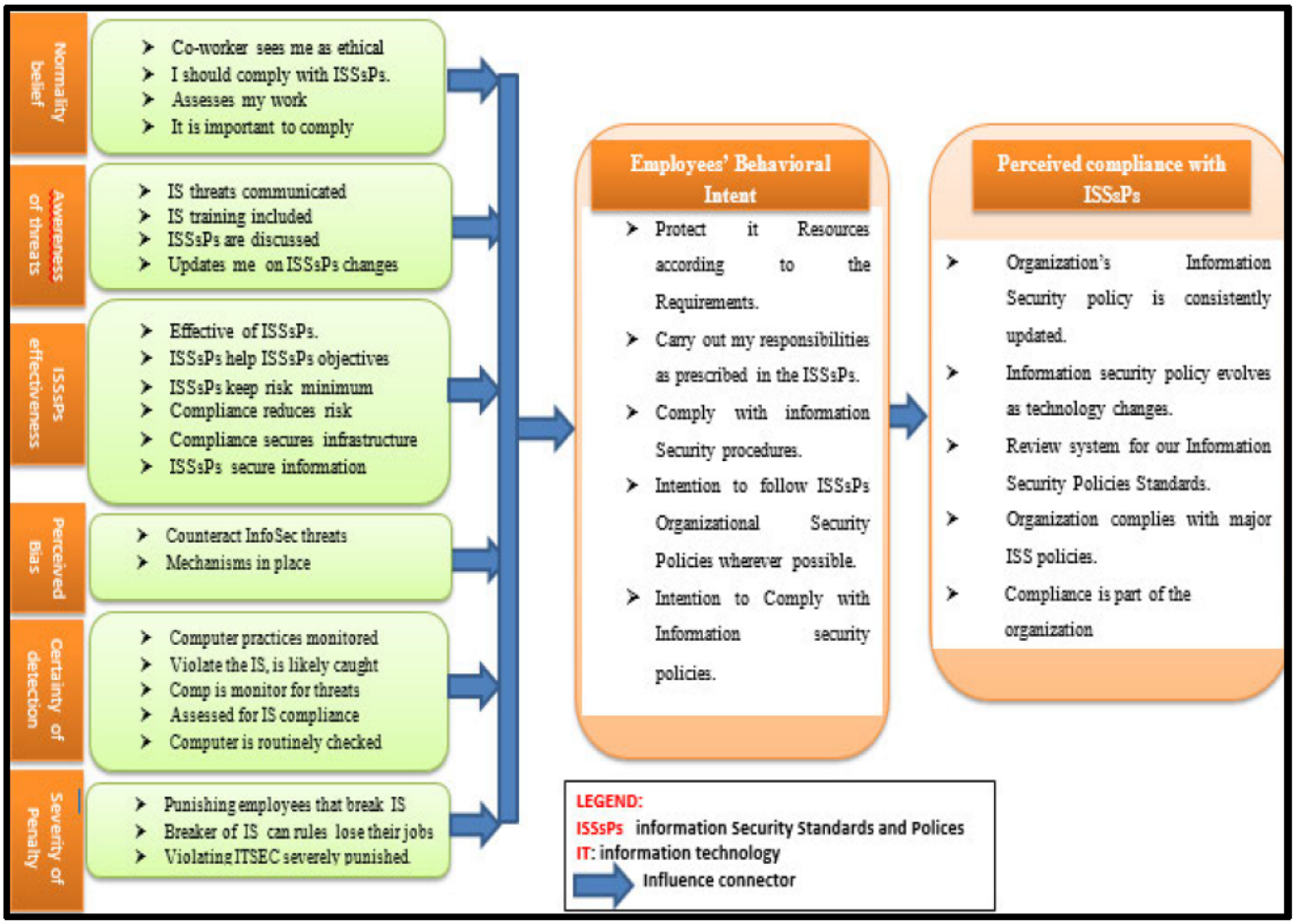


Figure 7.22: Employees' Information Security Standards and Policies Compliance Framework

7.11 **Implementation of the Framework**

It is important to note that this study is concerned with employee behaviour in term of complying with the ISSsPs. Management should familiarise themselves with the factors (normative, severity of penalty, certainty of detection, perception bias, perceived ISSsPs compliance and awareness of information security threats) that promote compliance with standards and policies in order to communicate this across the branches of the banks. A meeting should be held on how this can be integrated into the policies and how this can be

maintained. Operations managers and executive managers are to do the follow-up to ensure the proper implementation and practice of the content of the framework in order to ensure its compliance. ICT personnel and systems maintenance officers are to train employees to notify them of the compliance with ISSsPs, its importance and the consequences if not carried out as stated in the PMT. Additionally, intention to comply is a very important element amongst the motivational factors. Intention may not really mean the actual compliance as a process of conceiving a particular action, but the intention of the employee is to be motivated either by punishing the offender, which will serve as deterrence to others, or the co-workers comply with ISSsPs- which others will follow. The banks' executives should take the ISSsPs and write it in the form of a code of conduct. The monitoring team should ensure there is effectiveness in compliance with ISSsPs. If the compliance is effective and positive,employees will likely see compliance as a culture in their organisations.

CHAPTER EIGHT
SUMMARY, CONCLUSION AND RECOMMENDATION

8.0 Introduction

This chapter presents a summary of the research and its major findings. Moreover, the chapter recapitulates on the achievement of the research objectives, as well as the contribution of the study to the body of knowledge. The limitations of the study and useful recommendations on the way forward also form part of the chapter.

8.1 Recapitulation of the Achievement of Research Objectives

The increase in information security breaches has been reported to be alarming, resulting in organisations incurring colossal losses. Evidence shows that Nigerian banks depend mainly on information technology in combating cybercrime, thereby neglecting the employees' behavioural factors in curtailing information security breaches. Past studies focused on the adoption of ICT to combat cyber fraud; a sociological perspective on the youth's involvement in cyber fraud; the role of law and the criminal code in preventing cyber theft; and the negative effect of financial crime on banking performance and the Nigerian economy. Others highlighted the importance of information security compliance in preventing cyber fraud. However, none of these studies investigated the extent to which Nigeria complies with the standards and polices and the employees' behavioural factors that contribute to employee compliance with Information Security Standards and Policies in Nigerian banks.

The adoption and compliance of banks with information security standards and policies provides useful information for combatting information security threats and cyber security. In addition, adherence to information security by employees is one of the major ways of combatting cybercrime. In contributing to the body of knowledge, this study aimed to establish the extent of individual Nigerian banks' compliance rates, and investigated the influence of compliance rates and experiences of information security breaches, as well as the role of employee motivational factors in ensuring compliance with ISSsPs. In the conclusion the study proposed the **employees' compliance framework,** which in turn will be used in combatting information cybercrime. In the next section, a discussion based on the four objectives of the research questions and hypotheses is provided.

In achieving the goal of the research, the four directions (objectives) of the research are recapitulated next.

8.2 Objective One

> "*To examine the rate and extent to which Nigerian banks have complied with international information security codes and standards."*

This study identified Nigerian commercial banks' compliance rates with international standards and codes. A majority of the participants acknowledge that Nigerian banks review their standard once a year. Information security incidents are evident in the Nigerian banking sector today, as the technology adoption is increasing. This is the reality because in many organisations (e.g. banking sector), the speed and capacity of data consumption is more considered than security and the privacy of the customers. Past studies noted that the cybercrime facing Nigerian banks today is caused by low compliance with information security standards and policies. Complying with information security standard and policies is necessary as a means of combatting the cyber security challenges in the banking sector. Information security standards provide the systematic guidelines and accurate security information to successfully prevent and reduce cybercrime and also provides a strong defence. Hence, the study contributes to in filling the gap unattended to by other studies. This study identified Nigerian commercial banks' compliance rates with international standards and codes.

Compliance with information security should be the culture of the banking sector since the standards and policies provide useful information and guidelines that will help in combatting cybercrime in Nigeria's banking sector. To combat information security challenges as reported earlier, priority should be given to regular reviews of standards, which should be made mandatory.

Cybercrime is a global issue. Consequent to this, Nigerian banks are making frantic efforts to combat the prevalent vices. This is seen in the results of the research indicating that Nigerian banks give subscription to FISMA, HIPAA, SOX, ISO/IEC 17799, and GLBA, while these are given a renewal drive at least once a year.

8.3 Objective Two

"To determine the influence of compliance rates on experiences of perceived information security breaches."

The second objective observed the *influence of compliance rates on experiences of perceived information security breaches. As* the information security change increases, the tools to combat it should also increase. It was nevertheless found by the study that there is a positive influence of information security compliance rates on information security breaches, based on the responses of the respondents and as shown in the analysis. It is denoted that as information security compliance increases at a certain time, the perceived information security breaches are expected to decrease, and vice versa. In the research questions, respondents were asked to indicate their opinions regarding the research questions thus:

- *How often does your organisation experience information security breaches?*
- *When last did your organisation successfully avert a pending information security breach?*
- *Which of the following international ISSsPs, in your experience, successfully prevent an information security breach?*

In relation to the first question, more respondents acknowledged that their banks experience information security breaches at least once in a year. Indicatively, a majority of the banks in Nigeria are faced with information security challenges. The experience of information security breaches in Nigeria may be due to the lack of information security standards compliance, as it has been noted from the literature that ISSsPs contains guidelines, which if dutifully followed, ISSsPs are capable of reducing information security breaches.

As per the second question, a significant portion of the respondents showed that their organisations averted information security breaches more than a year previously, whilst some respondents indicated that their banks averted pending information security breaches between six months and a year previously, whilst still others agreed that their banks never averted any pending information security breaches. It is obvious that there are information security challenges and impending information breaches in the Nigerian banks.

The third question borders on the successful prevention of information security breaches through international ISSsPs. A small portion of the respondents indicated the strength of FISMA, HIPAA, SOX and GLBA in the successful prevention of information security breaches. Following up on the potential of the above-mentioned standards, ISO/IEC 17799 has received a higher poll in the prevention drive. With the opportunity given to the respondents to mention other standards, this has made them give consideration to other standards (ISO/IEC 27001, ISO 27002), in which they indicated the potentiality of the duo in preventing information security breach. Obviously, with the results obtained from banks in south-west Nigeria, preference is still given to ISO/IEC 17799 as a measure to combat information breaches, while emphasis was laid that it has successfully prevented information security breaches. However, though attention cannot be drawn away from the fact that ISO/IEC 17799 had a revised portion in 2005.

8.4 Objective Three

"*To investigate employee motivational factors which contribute to bank employees' intention to comply with international information security codes and standards, and their impacts on organisational compliance."*

In preserving the customer's information, the compliance of employees with ISSsPs is inevitable. This study explored the factors that contribute to information security policies and standards compliance, using the TPB, PMT and Self-efficacy theories. Consequently, theoretical studies have also examined employees' motivational factors, otherwise known as behavioural factors, but not comprehensively enough in highlighting the factors that motivate employees' compliance, in order to evaluate the intention to comply with ISSsPs, and improve organisational compliance. Such motivational factors,,which include severity of penalty, certainty of detection, normative beliefs, perceived effectiveness of ISSsPs, awareness of information security threats and perception biases, are treated individually. However, it was found that these elements have an influence on ISSsPs. Moreover, in evaluating this factor, further factor analysis was conducted and some items in the framework were dropped.

8.5 Objective Four

"To propose an employee compliance framework that highlights the compliance behaviour of employees in the Nigerian banking sector."

It is essential to note that one of the reasons for the study is to develop an employees' compliance framework that will address the insider threats, which will in turn reduce cybercrime in Nigeria's banking sector. In order to bring to reality the development of this employees' compliance framework, the factors motivating the compliance of employees with ISSsPs were critically explored. The influences of the individual factors on the ISSsPs are put into examination. It was found that all the factors influence ISSsPs.

The exploratory factor analysis test was conducted to examine the significance of the items of each individual motivational factor. During and after EFA, some factors could not load significantly into the framework and therefore they were dropped, while those that are significant were retained. There were forty-eight (48) items involved in the process. The returning items were thirty-five (35). Table 5.42 and Table 5.43 presents the outcome of the analysis with the retained items. Based on the outcome of the exploratory factor analysis conducted, the items which were significant were used to develop the framework. Figure 7.22 presents the **employees' compliance framework** after considering the individual influence on the ISSsPs. The study further seeks the opinions of high-ranking Nigerian bank employees regarding the credibility, flexibility and the cost-effectiveness of the framework and its suitability for implementations in their respective banks.

8.6 Implications

The findings of this study have important implications for policy-makers, academics as well as practitioners in the banking industry.

8.6.1 Theoretical Implications

Theoretically, this study contributed to the body of knowledge by investigating the concept of information security compliance in the banking industry in a developing country. It expanded on the existing literature, and conceptualised the empirically investigated ISSsPs compliance in the Nigerian banking industry. Its distinct contribution was by providing a framework that enhances an understanding of the motivational factors of ISSsPs compliance through the mediating effect of employees' behavioural intention.

This study also revealed that normative beliefs, information security threat awareness, perceived effectiveness of ISSsPs compliance, perception biases, certainty of detection and severity of penalty have a positive effect on ISSsPs compliance. Furthermore, it showed that

there is a mediating effect of employees' behavioural intention between the motivational factors and ISSsPs compliance. Hence, the study ascertained the theoretical underpinnings and provided evidence to support the TPB, self-efficacy theory and PMT.

8.6.2 Practical Implications

Nigerian banks have experienced increased levels of cyber fraud. While many studies have investigated this issue, none have highlighted the extent of cybercrime amongst Nigerian banks. This study thus makes a significant contribution by investigating the extent of Nigerian bank employees' compliance with information security policies and standards as it is currently experienced, and its role in preventing insider threats and cybercrime amongst these banks. It was noted that, in line with the Central Bank's requirements, Nigerian banks review their standards at least once a year. Despite the degree of compliance, cybercrime has not been totally curbed. This suggests that management should review these standards more frequently, while at the same time, the CBN should enforce compliance with international information security policies and standards for all the banks, with regular reviewing of the standards and codes. The factors that motivate employees' compliance are also important, hence bank management should use these to enhance compliance.

The study also explained the motivational factors of ISSsPs compliance amongst employees in the Nigerian banking industry. It brought together and investigated the relationship amongst the motivational factors, employees' behavioural intention and ISSsPs compliance to provide a comprehensive framework for information security compliance amongst Nigerian banking employees, thereby providing banking practitioners and policy-makers with valuable information when considering how to manage ISSsPs compliance amongst employees as a way of reducing insider threats and cybercrime.

8.6.3 Managerial Implications

The study found that certainty of detection, normative beliefs, awareness of information security threats and perception biases of information security threats influence ISSsPs compliance. This suggests that IT managers and security units in the Nigerian banking industry need to raise awareness amongst employees about the impact of information security breaches on the well-being of the organisation. In delivering this message, IT managers and heads of operations should participate in departmental meetings, and awareness sessions/seminars to

reiterate these points. Furthermore, IT managers, heads of operations and maintenance managers in the Nigerian banking industry should endeavour to write ISSsPs in clear, unambiguous, easy-to-read and understandable language. Staff should receive information security training to increase their confidence in their ability to comply with the standards and policies and to easily identify insider threats.

8.6.4 Implication of the Framework

This research examined ISSsPs compliance by integrating three appropriate theories, namely the TPB, the PMT and the self-efficacy theory. The study showed that motivational factors, otherwise known as behavioural factors (severity of penalty, certainty of detection, normative beliefs, awareness of information security threats and perception bias), influence employees' compliance intentions. The responses of the respondents indicated that the framework is good for implementation across the branches of the selected banks. Moreover, the outcome indicated that the framework is flexible and cost-effective. There is therefore much assurance that the right implementation of the framework will enhance the compliance rate of employees with ISSsPs in the Nigerian banking sector. It is important to note that there is always a behavioural change at a particular time as technology changes occur. It is therefore imperative that the framework should be regularly reviewed and additional content that can promote employees' compliance should be added as the framework is regularly reviewed.

8.7 Limitations and Suggestions for Future Studies

As with any empirical study, this study has limitations that should be considered when interpreting the results. Data collection was geographically confined to the banking sector in the South-west geopolitical zone of Nigeria. Hence, in generalising the study's findings, future studies should consider the socio-cultural differences which may be of interest to multinational firms. Incorporating the socio-cultural differences within which the industry operates may enrich the findings of future studies and will increase the generalisability of the results.

Furthermore, a cross-sectional design was used, which requires that primary data is gathered at a point in time during the study. This could limit its ability to show information compliance trends in the banking industry over time. Employee perceptions of information security may also change over time. Therefore, future studies could consider a longitudinal design to reveal information security compliance trends. It should be noted that the responses to the question

on how often the banks review their standards are based on the study participants' perceptions. However, from the results, there is an indication that ISO/IEC 17799 as still in the banking systems in Nigeria when the standard has been re-rewritten since 2005. Hence further research should investigate the reason Nigerian commercial banks preferred the old standards rather than the ISO/IEC27002 and ISO/IEC 27001 when ISO/IEC27002 and ISO/IEC 27001 covers the major information security of the organisation and provides useful information for combatting cybercrime.

Although the literature contends that intention is the most proximal influence on behaviour, it is not guaranteed that employees will behave as indicated. Even though there is sound empirical evidence that employees' intentions to comply with ISSsPs have a significant impact on actual compliant behaviour, future research should re-assess the research framework, measuring actual behaviour. Another avenue for further research is to consider the effect of moral reasoning, since an individual's moral commitment has been found to influence information misuse intention. The response from the respondents during the validation is very useful in terms of an exploration of the human factor for combatting insider threats. Continual commitment, training and regular review are not considered in this study. Therefore, further research should endeavour to include this element.

8.8 Conclusion

This study empirically revealed the links and relationships amongst its variables and tested these relationships both directly and indirectly in order to provide answers to the research questions and achieve the corresponding research objectives. Upon validation of the research instrument, data were collected from the employees of banks in the South-western zone of Nigeria. The data were initially subjected to a series of analytical procedures and finally analysed using SPSS software version 25. Nonetheless, both descriptive and inferential statistical analyses were conducted to achieve the study's objectives and evidence was found to support the results of the analysis.

This study empirically revealed the extent and level of information security compliance amongst employees in the Nigerian banking industry, thus achieving objective one. The findings show that ISSsPs in the Nigerian banking industry are reviewed at least once every year, and that there is commitment amongst bank employees to maintain information security

compliance. The study further concluded that information security policies and standards are frequently updated by Nigerian banks to keep up with rapid changes in technology.

The study's second objective was to determine the relationship between compliance rates and experiences of perceived information security breaches in the Nigerian banking industry. This was achieved through descriptive analysis. A positive relationship was established between the banks' review of ISSsPs compliance and experiences of information security breaches. This implies that the rate of information security breaches experienced by banks will increase the rate of compliance with ISSsPs. This also indicate the employees' importance of compliance.

The third objective of this study was to investigate the employee motivational factors which contribute to bank employees' intention to comply with information security codes and standards. In achieving this objective, it was found that the severity of penalties meted out to employees, certainty of detection, normative beliefs, perceived effectiveness of security, perception bias and security threat awareness contribute to employees' intention to comply with information security codes and standards. Furthermore, it was found that employees' behavioural intention plays an important mediating role between the motivational factors and employees' information security compliance intention, as it mediates the relationships between these motivational factors and ISSsPs compliance.

Proposing an ISSsPs compliance framework to reduce experiences of cyber theft and fraud amongst Nigerian banks was the fourth objective of this study. This framework was developed using the overall results of the factor analysis, whereby the items which are not significant were dropped, while the significant items are retained and used. The individual influence of employee motivational factors on compliance with ISSsPs to indicate the dynamic compliance of employees with ISSsPs was also considered. The framework shows that the factors highlighted are predictors of employees' compliance with ISSsPs, which in turn reduces the rate of cyber fraud and information security breaches in the Nigerian banking industry.

In summary, the following important theoretical gaps were identified in the literature and were filled by this study:

i. Although the CBN report (2014) praised Nigerian apex banks for complying with ISO/IEC 27001, no substantial and corresponding acknowledgement of such compliance has been reported for mainstream Nigerian commercial banks, or for other

international standard codes like FISMA, HIPAA, SOX, ISO/IEC 17799 and GLBA. Hence, this study identified Nigerian commercial banks' compliance rates with individual international standards and codes.

ii. Previous studies on information security in the Nigerian banking industry have not validated the hypothetical claim that compliance with international ISSsPs reduces the experience of cyber theft. This study empirically investigated the relationship between Nigerian banks' compliance rates and experiences of information security breaches. It was noted that compliance rate has a relationship with information security breaches.

iii. Employees play a significant role in ensuring organisational efficiency and in this case, organisational compliance with international ISSsPs, while the motivational factors that contribute to employees' intention to comply have not been comprehensively investigated. This study filled this gap by investigating the motivational factors that contribute to employee compliance with ISSsPs, as well as their theoretical underpinnings.

iv. The study developed a framework which highlights the ISSsPs compliance dynamic of Nigerian bank employees. The paradigm combines elements from the protection motivation theory, the self-efficacy theory and the theory of planned behaviour. The framework was evaluated by high-ranking experts in the banking sector. The validation was based on the appropriateness, feasibility in relation to cost-saving, timing and resources, flexibility in the usage of the framework, as well as intention to use. It is believed that when the dynamic compliance of employees is known and this framework is implemented by organisations, the resultant effect will bring a reduction in insider threats, which in turn will reduce cybercrime in Nigerian banks.

v. As an addition to the body of knowledge, this study focuses on the conceptual principles of information security standards and policies compliance amongst Nigerian bank employees, while it offers practical guidelines and theoretical reasons for improving employee compliance with information security policies. The theoretical study focused on the theories that promote an understanding on how compliance can be improved. Empirical studies on information security standards and policies compliance are useful because they are grounded on both theoretical and empirical validation.

REFERENCES

Abawajy, J. (2014). User Preference of Cyber Security Awareness Delivery Methods. *Behaviour and Information Technology*, *33*(3), 237-248.

Abazari, F., Takabi, H. and Analoui, M. (2019). *Security, Privacy, and Digital Forensics in the Cloud*, 129-141. New Jersey, USA. Wiley Online Library.

Abelson, H., Anderson, R., Bellovin, S. M., Benaloh, J., Blaze, M., Diffie, W., …… Weitzner, D. J. (2015). *Keys Under Doormats: Mandating Insecurity by Requiring Government Access to all Data and Communications. Journal of Cybersecurity*, *1*(1), 69-79.

Abubakar, A. (2014). The Effects of Electronic Banking on Growth of Deposit Money Banks in Nigeria. *European Journal of Business and Management* 6(33), 79-89.

Acuna, E. and Rodriguez, C. (2004). The Treatment of Missing Values and its Effect on Classifier Accuracy. In *Classification, Clustering, and Data Mining Applications* (pp. 639-647). Springer, Berlin, Heidelberg.

Adesugba, M. A., and Mavrotas, G. (2016). Delving Deeper into the Agricultural Transformation and Youth Employment Nexus: *The Nigerian Case* (Vol. 31). Intl Food Policy Res Inst.

Afzal, S., Arshad, M., Saleem, S. and Farooq, O. (2019). The Impact of Perceived Supervisor Support on Employees' Turnover Intention and Task Performance: Mediation of Self-Efficacy. *Journal of Management Development*. 1-16. Available at https://doi.org/10.1108/JMD-03-2019-0076

Aghware, F. O. and Egbuna, E. O. (2012). People Centred Information Security Model for Corporate Nigeria. *Proceedings of the World Congress on Engineering and Computer Science,* Vol. 1 WCECS 2012, October 24-26, 2012, San Francisco, USA.

Ajayi, E. F. G. (2016). The Impact of Cybercrimes on Global Trade and Commerce. *International Journal of Information Security and Cybercrime (IJISC), 5*(2), 31-50.

Akamai (2015). *Commonly Accepted Security Practices and Recommendations (CASPR)*. A White Paper Report on Information Security Compliance

Akinbowale, O. E., Klingelhöfer, H. E., and Zerihun, M. F. (2020). Analysis of Cyber-crime Effects on the Banking Sector Using Balance Score Card: A Survey of Literature. *Journal of Financial Crime*.

Akinyomi, O. J. (2012). Examination of Fraud in The Nigerian Banking Sector and its Prevention. *Asian Journal of Management Research*, *3*(1), 182-194.

Al-Alami, L., 2011. *Membership in Social Networks and its Effect on Improving Political Awareness of Al-Najah University Students.* (Postgraduate Thesis). Al- Najah University, Palestine.

Alber, N. and Nabil, M. (2016). The Impact of Information Security on Banks' Performance in Egypt. *International Journal of Economics and Finance*. 7(9). 219-225.

Al-Dmour, R., Dawood, E. A. H., Al-Dmour, H., and Masa'deh, R. E. (2020). The Effect of Customer Lifestyle Patterns on the Use of Mobile Banking Applications in Jordan. *International Journal of Electronic Marketing and Retailing*, *11*(3), 239-258.

Al Hogail, A. and AlHogail, A. (2015). Cultivating and Assessing Organisational Information Security Culture, an Empirical Study. *International Journal of Security and Its Applications*, *9*(7), 163-178.

AlKalbani, A., Deng, H. and Kam, B. (2019, June). The Influence of Organisational Enforcement on the Attitudes of Employees Towards Information Security Compliance. In *2019 10th International Conference on Information and Communication Systems (ICICS)* (pp. 152-159). IEEE.

Alshaikh, M., Naseer, H., Ahmad, A. and Maynard, S. B. (2019). "Toward Sustainable Behaviour Change: An Approach for Cyber Security Education Training and Awareness". *In Proceedings of the 27th European Conference on Information Systems (ECIS)*, Stockholm and Uppsala, Sweden, June 8-14, 2019. ISBN 978-1-7336325-0-8 Research Papers.

Albrechtsen, E. (2015). Major Accident Prevention and Management of Information Systems Security in Technology-Based Work Processes. *Journal of Loss Prevention in the Process Industries*, *36*, 84-91.

Albrechtsen, E. and Hovden, J. (2009). The Information Security Digital Divide Between Information Security Managers and Users. *Computers and Security, 28*(6), 476-490.

Albrechtsen, E., and Hovden, J. (2010). Improving Information Security Awareness and Behaviour Through Dialogue, Participation and Collective Reflection. An Intervention Study. *Computers and Security, 29*(4), 432-445.

Alese, B. K., Thompson, A. F., Owa, K. V., Iyare, O. and Adebayo, O. T. (2014). Analysing Issues of Cyber Threats in Nigeria. *In Proceedings of the World Congress on Engineering 2014 Vol I, WCE 2014*, July 2 - 4, 2014, London, U.K

Ali, L. (2019). CyberCrimes-A Constant Threat for the Business Sectors and its Growth (A Study of the Online Banking Sectors in GCC). *The Journal of Developing Areas*, *53*(1), 267-279.

Alnatheer, M. A. (2015). Information Security Culture Critical Success Factors. In *2015 12th International Conference on Information Technology-New Generations* (pp. 731-735). IEEE.

AlHogail, A. (2015). Design and Validation of Information Security Culture Framework. *Computers in Human Behavior*, *49*, 567-575.

AlKalbani, A., Deng, H., Kam, B., and Zhang, X. (2016). Investigating the Impact of Institutional Pressures on Information Security Compliance in Organisations. *Australasian Conference on Information Systems 2016, Australia, Wollongong*.

Alotaibi, M. J., Furnell, S., and Clarke, N. (2019). A Framework for Reporting and Dealing with End-user Security Policy Compliance. *Information and Computer Security*, 27(1), pp. 2-25.

Alzahrani, A., Johnson, C. and Altamimi, S. (2018, May). Information Security Policy Compliance: Investigating the Role of Intrinsic Motivation Towards Policy Compliance in the Organisation. In *2018 4th International Conference on Information Management (ICIM)* (pp. 125-132). IEEE.

Amarachi, A. A., Okolie, S. O., and Ajaegbu, C. (2013). Information Security Management System: Emerging Issues and Prospect. *IOSR Journal of Computer Engineering*, *12*(3), 96-102.

Ameen, N., Tarhini, A., Shah, M. H., and Madichie, N. O. (2020). Employees' Behavioural Intention to Smartphone Security: A Gender-based, Cross-National Study. *Computers in Human Behavior*, *104*, 106184.

Anderson, A., and Barton-Wales, S. (2019). Musical Culture and the Primary School: An Investigation into Parental Attitudes to Whole Class Ensemble Teaching in the English

Primary School and Potential Impacts on Children's Musical Progress. *British Journal of Music Education*, *36*(3), 267-279.

Anderson, Ross, Barton, Chris, Bölme, Rainer, Clayton, Richard, Gañán, Carlos, Grasso, Tom, Levi, Michael, Moore, Tyler and Vasek, Marie 2019. Measuring the changing cost of cybercrime. Presented at: *The 2019 Workshop on the Economics of Information Security*, Boston, US, 3-4 Jun 2019.

Apuke, O. D. (2017). Quantitative Research Methods a Synopsis Approach. *Kuwait Chapter of the Arabian Journal of Business and Management Review*, *6*(11), 40-47.

Asekome, M. O., and Abieyuwa, A. J. (2014). Challenges of Banking Sector Reforms in Nigeria: An Appraisal. *International Journal of Business and Social Science*, *5*(7), 1.

Ashenden, D. (2018). Information Security Management: A Human Challenge? *Information Security Technical Report, 13*(4), 195-201

Asheri, C. J., Louise, Y., and Stewart, K. (2012). *Security Metrics and Evaluation of Information Systems Security.* Department of Computer and Systems Sciences, Stockholm University/KTH Forum 100, 16440 Kista, Sweden.

Atiku, S. O., and Fields, Z. (2017). Banking Policy, Banks Efficiency and Job Security in Nigeria. *Journal of Business and Retail Management Research*, *11*(3).

Aulakh, P. S. and Gencturk, E. F. (2000). International Principal–Agent Relationships: Control, Governance and Performance. *Industrial Marketing Management*, *29*(6), 521-538.

Aydin, C. E. and Rice, R. E. (1991). Social Worlds, Individual Differences, and Implementation: Predicting Attitudes Toward a Medical Information System. *Information and Management*, *20*(2), 119-136.

Aytes, K. and Connolly, T. (2004). Computer Security and Risky Computing Practices: A Rational Choice Perspective. *Journal of Organisational and End User Computing (JOEUC)*, *16*(3), 22-40.

Babbie, E. (2010). The Practice of Social Research-12. *Belmont: Wadsworth*.

Badie, N. and Lashkari, A. H. (2012). A New Evaluation Criterion for Effective Security Awareness in Computer Risk Management Based on AHP. *Journal of Basic and Applied Scientific Research*, *2*(9), 9331-9347.

Badshah, I., Koerniadi, H. and Kolari, J. (2019). The Sarbanes-Oxley Act and Informed Trading in the Options Market: Evidence from Share Repurchase Announcements. *International Review of Finance.* Available @ https://onlinelibrary.wiley.com/doi/epdf/10.1111/irfi.12281.

Bahuguna, A., Bisht, R. K., and Pande, J. (2018, July). Roadmap Amid Chaos: Cyber Security Management for Organisations. In *2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT)* (pp. 1-6). IEEE.

Baik, N. (2017). *An Empirical Study on the Impact of Penalty Charges To Customer Repurchase Behaviour – Airlines Penalty Cases in South Korea*–Doctorate Thesis, Brunel University, London).

Bamberg, S., Rollin, P., and Schulte, M. (2020). Local Mobility Culture as Injunctive Normative Beliefs–A Theoretical Approach and a Related Measurement Instrument. *Journal of Environmental Psychology*, 101465

Bandura, A. (1977). Self-efficacy: Toward a Unifying Theory of Behavioral Change. *Psychological Review*, *84*(2), 191.

Bandura, A. (1986). *Social Foundation of Thought and Action: A Social-Cognitive View.* Englewood Cliffs.

Bandura, A. (2010). Self-efficacy. *The Corsini Encyclopedia of Psychology*, 1-3.

Bandura, A. and Locke, E. A. (2003). Negative Self-Efficacy and Goal Effects Revisited. *Journal of Applied Psychology*, *88*(1), 87.

Baskerville, R., Spagnoletti, P., and Kim, J. (2014). Incident-Centered Information Security: Managing a Strategic Balance Between Prevention and Response. *Information and Management*, *51*(1), 138-151.

Bauer, S., and Bernroider, E. W. (2017). From Information Security Awareness to Reasoned Compliant Action: Analyzing Information Security Policy Compliance in a Large Banking Organisation. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems*, *48*(3), 44-68.

Bell, A. J., Rogers, M. B. and Pearce, J. M. (2019). The Insider Threat: Behavioral Indicators and Factors Influencing Likelihood of Intervention. *International Journal of Critical Infrastructure Protection*, *24*, 166-176.

Bell, E., Bryman, A. and Harley, B. (2018). *Business Research Methods*. Oxford University Press. Available @

Benaroch, M., Lichtenstein, Y. and Robinson, K. (2006). Real Options in Information Technology Risk Management: An Empirical Validation of Risk-Option Relationships. *MIS Quarterly*, 827-864.

Best, B. B. (2014). Influencing Employees' Compliance Behavior Towards Information Security Policy Masters of Business Administration (MBA) *at the Maastricht School of Management (MsM), Maastricht, the Netherlands*,

Bedford, J. and Van Der Laan, L. (2016). Organisational Vulnerability to Insider Threat. In *International Conference on Human-Computer Interaction* Springer, Cham (pp. 465-470).

Bianchi, G., Caponi, A., Pisa, C., Stammati, L., Dargahi, T., Cut, M. S., . . . Vavoulas, N. (2012). From Real-world Identities to Privacy-preserving and Attribute-based Credentials for Device-centric Access Control. *Deliverable D5*. Available @ https://www.recred.eu/sites/default/files/recred_d5.2.pdf.

Blakley, B., McDermott, E., and Geer, D. (2001). Information Security is Information Risk Management. In *Proceedings of the 2001 Workshop on New Security Paradigms* (pp. 97-104). ACM.

Bowen, P., Rose, R. and Pilkington, A. (2017). Mixed Methods-Theory and Practice. Sequential, Explanatory Approach. *International Journal of Quantitative and Qualitative Research Methods*, 5, 10-27.

Brown, E. A. (2017). Workplace Wellness: Social Injustice. *NYUJ Legis. and Pub. Pol'y*, *20*, 191.

Brown, J. D. (2011). Likert Items and Scales of Measurement. *Statistics*, *15*(1), 10-14.

BSI (2015). Central Bank of Nigeria to deliver the highest standard of Information Security. Retrieved from http://www.bsigroup.com/LocalFiles/enAE/Case%20Studies/ISO%20ISO/IEC ISO/IEC 27001%20Case%20studies/ISO%20ISO/IEC ISO/IEC 27001_Central_Bank_NigeriaCase%20Study%20LOWRES.pdf, on 7th October, 2015.

Bulgurcu, B., Cavusoglu, H. and Benbasat, I. (2009). Roles of Information Security Awareness and Perceived Fairness in Information Security Policy Compliance. *AMCIS 2009 Proceedings*, 419.

Bulgurcu, B., Cavusoglu, H. and Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *MIS Quarterly*, *34*(3), 523-548.

Brunner, M., Sauerwein, C., Felderer, M., and Breu, R. (2020). Risk Management Practices in Information Security: Exploring the Status Quo in the DACH Region. *Computers and Security*, 101776.

Burns, A. J. (2019). Security Organizing: A Framework for Organisational Information Security Mindfulness. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems*, *50*(4), 14-27.

Cameron, K. S., and Whetten, D. A. (2013). *Organisational Effectiveness: A Comparison of Multiple Models*. United Kingdom, NY City: Academic Press.

Carden, S., Camper, T. and Holtzman, N. (2019). Cronbach's Alpha Under Insufficient Effort Responding: An Analytic Approach. *Stats*, *2*(1), 1-14.

Catteddu, (2010). Cloud Computing: Benefits, Risks and Recommendations for Information Security. In *Web Application Security* (pp. 17-17). Springer: Berlin, Heidelberg.

Cavelty, M. D. (2007). *Cyber-Security and Threat Politics: Us Efforts to Secure The Information Age*: Routledge.

Cavelty, M. D. (2015). Cyber-Security and Private Actors. *Routledge Handbook of Private Security Studies*, (1) 89-99.

Cavusoglu, H., Cavusoglu, H., Son, J. and Benbasat, I. (2009). Information Security Control Resources in Organisations: A Multidimensional View and Their Key Drivers. *UBC Working Paper*.

Central Bank of Nigeria (CBN) (2014). CBN Maintains Highest Level in ISS (ISOISO/IEC ISO/IEC 27001) Compliance, Retrieved from https://www.cbn.gov.ng/out/2014/ccd/cbn-iso.pdf on 7th October, 2016.

Cerna, L. (2013). The Nature of Policy Change and Implementation: A Review of Different Theoretical Approaches. Organisation for Economic Cooperation and Development (OECD) Report, Geneva, Switzerland.

Chan, Y. E., Sabherwal, R. and Thatcher, J. B. (2006). Antecedents and Outcomes of Strategic IS Alignment: An Empirical Investigation. *IEEE Transactions on Engineering*

Management, *53*(1), 27-47.

Chandrashekhar, A. M., Muktha, G. S. and Anjana, D. K. (2016). Cyberstalking and Cyberbullying: Effects and Prevention Measures. *Imperial Journal of Interdisciplinary Research*, *2*(3), 95-102.

Chang, L. Y., and Coppel, N. (2020). Building Cyber Security Awareness in A Developing Country: Lessons from Myanmar. *Computers and Security*, 101959.

Cheng, L., Li, Y., Li, W., Holm, E. and Zhai, Q. (2013). Understanding the Violation of IS Security Policy in Organisations: An Integrated Model Based on Social Control and Deterrence Theory. *Computers and Security*, *39*, 447-459.

Chen, T., Hammer, J., and Dabbish, L. (2019, May). Self-Efficacy-based Game Design to Encourage Security Behaviour online. In *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems* (pp. 1-6).

Chester, R., Khondoker, M., Shepstone, L., Lewis, J. S. and Jerosch-Herold, C. (2019). Self-Efficacy and Risk of Persistent Shoulder Pain: Results of a Classification and Regression Tree (CART) Analysis. *British Journal of Sports Medicine*, *53*(13), 825-834.

Chevalier, A., Charlemagne, M., and Xu, L. (2020). Data on Public Bicycle Acceptance Among Chinese University Populations. *Data in Brief*, *28*, 104946.

Chevers, Delroy A. (2019). The Impact of Cybercrime on E-banking: A Proposed Model. CONF-IRM 2019 (p. 11).

Chiu, C. M., and Tan, C. M. (2020). Enhancing Employees' Intention to Comply with Information Security Policies: The Roles of Job Crafting and Organisational Commitment. In *PACIS* (p. 166).

Choi, K. S., Cho, S. and Lee, J. R. (2019). Impacts of Online Risky Behaviours and Cybersecurity Management on Cyberbullying And Traditional Bullying Victimization among Korean Youth: Application of Cyber-Routine Activities Theory with Latent Class Analysis. *Computers in Human Behavior*, *100*, 1-10.

Choi, S., Martins, J. T., and Bernik, I. (2018). Information Security: Listening to the Perspective of Organisational Insiders. *Journal of Information Science*, *44*(6), 752-767.

Choi, M. (2016). Leadership of Information Security Manager on The Effectiveness of Information Systems Security for Secure Sustainable Computing. *Sustainability*, *8*(7), 638.

Choi, M., Levy, Y. and Hovav, A. (2013). The Role of User Computer Self-Efficacy, Cybersecurity Countermeasures Awareness, and Cybersecurity Skills Influence on Computer Misuse. In *Proceedings of the Pre-International Conference of Information Systems (ICIS) SIGSEC–Workshop on Information Security and Privacy (WISP)*.

Chua, H. N., Wong, S. F., Low, Y. C. and Chang, Y. (2018). Impact of Employees' Demographic Characteristics on The Awareness and Compliance of Information Security Policy in Organisations. *Telematics and Informatics*, *35*(6), 1770-1780.

Clark, M., Espinosa, J., and Delone, W. (2020, January). Defending Organisational Assets: A Preliminary Framework for Cybersecurity Success and Knowledge Alignment. In *Proceedings of the 53rd Hawaii International Conference on System Sciences*.

Coffee Jr, J. C. (2020). *Corporate Crime and Punishment: The Crisis of Underenforcement*. Berrett-Koehler Publishers Oakland.

Coglianese, C., and Nash, J. (2020). Compliance Management Systems: Do They Make a Difference? *Cambridge Handbook of Compliance (D. Daniel Sokol and Benjamin Van Rooij Eds., Cambridge University Press, Forthcoming)*, 20-35.

Cohen-Louck, K., and Levy, I. (2020). Risk Perception of a Chronic Threat of Terrorism: Differences Based on Coping Types, Gender and Exposure. *International Journal of Psychology*, *55*(1), 115-122.

Collins, T. (2019). Towards the Computational Assurance of Integrity. Similar Systems: Found in Lawsection 4 (p.1-10).

Collis, J. and Hussey, R. (2003). *Business Research:* Palgarve Macmillan.

Colosi, H. A., Costache, C., and Colosi, I. A. (2019). Informational Privacy, Confidentiality and Data Security in Research Involving Human Subjects. *Applied Medical Informatics*, *41*, 16-16.

Colquitt, J. A., Greenberg, J., and Greenberg, J. (2003). Organisational Justice: A Fair Assessment of the State of the Literature. *Organisational Behavior: The State of the Science*, 159-200.

Colwill, C. (2009). Human Factors in Information Security: The Insider Threat – Who Can You Trust These Days? *Information Security Technical Report, 14*(4), 186-196.

Cox, J. (2012). Information Systems User Security: A Structured Model of the Knowing-Doing gap. *Computers in Human Behaviour, 28,* 1849-1858.

Creswell, J. W. and Poth, C. N. (2017*). Qualitative Inquiry and Research Design: Choosing Among Five Approaches*. Sage Publications.

Creswell, J. W. (2013). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. Sage Publications

Creswell, J.W. (2009). *Research Design: Qualitative, Quantitative and Mixed Methods Approaches.* Third Edition, United States of America: Sage.

Da Veiga, A., and Martins, N. (2015). Improving the Information Security Culture Through Monitoring and Implementation Actions Illustrated Through a Case Study. *Computers and Security, 49,* 162-176.

D'Arcy, J., Herath, T., and Shoss, M. K. (2014). Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective. *Journal of Management Information Systems, 31*(2), 285-318.

D'Arcy, J., Hovav, A. and Galletta, D. (2009). User Awareness of Security Countermeasures and its Impact on Information Systems Misuse: A Deterrence Approach. *Information Systems Research*, *20*(1), 79- 98.

Deloitte (2015). Nigerian Cyber Security Outlook 2015. *Insights*. Retrieved from http://www2.deloitte.com/ng/en/pages/risk/articles/nigerian-cyber-security-outlook-2015.html on 28th September, 2016.

Dhillon, P. M. S. (2017). Advanced Encryption Techniques Based on IOT (Internet of Thing). *International Journal for Computer Application and Research, IF 2.003, Einstein IF 4.873, 5*(4).

Diehl, E., Rieger, S., Letzel, S., Schablon, A., Nienhaus, A., Pinzon, L. C. E., and Dietz, P. (2020). Health and Intention to Leave the Profession of Nursing-Which Individual, Social and Organisational Resources Buffer the Impact of Quantitative Demands? A Cross-Sectional Study. *BMC Palliative Care*, *19*(1), 1-13.

Dissanayake, E. (2015). *What is art for?* University of Washington Press.

Dolnicar, S. (2020). Why Quantitative Papers Based on Primary Data Get Desk-Rejected by Annals of Tourism Research. *Annals of Tourism Research*, *83*, 102981.

Dourish, P., Grinter, E., Delgado De La Flor, J. and Joseph, M. (2004). Security in the Wild: User Strategies for Managing Security as an Everyday Practical Problem. *Personal and Ubiquitous Computing*, *8*(6), 391-401.

Downer, K., and Bhattacharya, M. (2015). BYOD Security: A New Business Challenge. Paper Presented at The IEEE International Conference on Smart City/Socialcom/Sustaincom (Smartcity: Chengdu, China. December 19-21, 2015.

Dutta, A. and Roy, R. (2008). Dynamics of Organisational Information Security. *System Dynamics Review: The Journal of the System Dynamics Society*, *24*(3), 349-375.

Ellis, D. A. (2019). Are smartphones really that bad? Improving the psychological measurement of technology-related behaviors. *Computers in Human Behavior*, *97*, 60-66.

Emeka, E. O. (2018). Cyber Crime in Nigeria: A review of Causes, Issues and Meeting the Challenges. *A African Journal of Science Education ISSN*, *1*(1).

Enoch, Y. S., John, A. K. and Olumuyiwa, A. E. (2013). Mitigating Cyber Identity Fraud Using Advanced Multi Anti-Phishing Technique. *International Journal of Advanced Computer Science and Applications*, *4*(3), 156-164.

Ehrlich, I. (1996). Crime, Punishment, and the Market for Offenses. *Journal of Economic Perspectives*, *10*(1), 43-67.

Eisenhardt, K. M. (1989). Agency Theory: An Assessment and Review. *Academy of Management Review*, *14*(1), 57-74.

Evans, M., He, Y., Maglaras, L., and Janicke, H. (2019). HEART-IS: A Novel Technique for Evaluating Human Error-Related Information Security Incidents. *Computers and Security*, *80*, 74-89.

Fabian, A. (2013). Corporate Governance and Ethical Business Dealings in Nigeria: The Imperatives "Business Day 21st February 2013. Retrieved from http://www.businessdayonline.com/NG/index.php/business-intelligence/51906-corporate-governance-and-ethical-business-dealings-in-nigeria-the-imperatives

Fadairo, O. S., Fadairo, A. O., and Aminu, O. (2014). Coverage of corruption news by major newspapers in Nigeria. *New Media and Mass Communication*, *24*, 53-59.

Fadare, O. A. (2015). Impact of ICT Tools for Combating Cyber Crime in Nigerian Online Banking: A Conceptual Review. *International Journal of Trade, Economics and Finance, 6* (5), October 2015, 272 – 277. doi: 10.18178/ijtef.2015.6.5.481.

Farahnak, L. R., Ehrhart, M. G., Torres, E. M., and Aarons, G. A. (2020). The Influence of Transformational Leadership and Leader Attitudes on Subordinate Attitudes and Implementation Success. *Journal of Leadership and Organisational Studies, 27*(1), 98-111.

Farr, M. and Bailey, D. (2019). Uniting Business Continuity Management and Operational Risk Management. *Journal of Business Continuity and Emergency Planning*, *12*(4), 294-300.

Fazlida, M. R., and Said, J. (2015). Information Security: Risk, Governance and Implementation Setback. *Procedia Economics and Finance*, *28*, 243-248.

Fernet, C., Trépanier, S. G., Austin, S., Gagné, M. and Forest, J. (2015). Transformational Leadership and Optimal Functioning at Work: On the Mediating Role of Employees' Perceived Job Characteristics and Motivation. *Work and Stress*, *29*(1), 11-31.

Ferreira, C., Merendino, A., and Meadows, M. (2019). How Big Data Can Destroy Organisations' Legitimacy. *Journal of Production Economics*, *97*, 1.

Fishbein, M. and Ajzen, I. (1975). *Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research*, 181-202.

Frank, I., and Odunayo, E. (2013). Approach to Cyber Security Issues in Nigeria: Challenges and Solution. *International Journal of Cognitive Research in Science, Engineering and Education*, *1*(1).

Fishbein, M., and Ajzen, I. (2011). *Predicting and Changing Behavior: The Reasoned Action Approach*. Psychology Press.

Frias-Aceituno, J. V., Rodriguez-Ariza, L., and Garcia-Sanchez, I. M. (2013). The Role of the Board in the Dissemination of Integrated Corporate Social Reporting. *Corporate Social Responsibility and Environmental Management*, *20*(4), 219-233.

Gangire, Y., Da Veiga, A., and Herselman, M. (2019, March). A Conceptual Model of Information Security Compliant Behaviour Based on the Self-Determination Theory. *In 2019 Conference on Information Communications Technology and Society (ICTAS)* (pp. 1-6). IEEE.

Garoupa, N. (2000). The Economics of Organized Crime and Optimal Law Enforcement. *Economic Inquiry*, *38*(2), 278-288.

Gates, S., Prachyl, C. L. and Sullivan, C. (2016). Using Report to the Nations on Occupational Fraud and Abuse to Stimulate Discussion of Fraud in Accounting and Business Classes. *Journal of Business and Behavioral Sciences*, *28*(1), 106.

Ghasemi, A. and Zahediasl, S. (2012). Normality Tests for Statistical Analysis: A Guide for Non-Statisticians. *International Journal of Endocrinology and Metabolism*, *10*(2), 486.

Ghauri, P., Grønhaug, K., and Strange, R. (2020). *Research Methods in Business Studies*. Cambridge University Press.

Gashi, F., and Peci, B. (2020). Protection of Personal Data and Privacy in Banking Sector In Kosovo and its Impact in Consumer Protection. *Perspectives of Law and Public Administration*, *9*(1), 70-78.

Gehrmann, M. (2012). Combining ITIL, COBIT and ISO/IEC 27002 for Structuring Comprehensive Information Technology for Management in Organisations. *Navus-Revista De Gestão E Tecnologia*, *2*(2), 66-77.

Ghouri, A. M., Khan, N. R. and Kareem, O. B. (2016). Improving Employees Behaviour through Extension in Theory of Planned Behaviour: A Theoretical Perspective for SMEs. *International Journal of Business and Management, 11*(11), 196-213.

Gibson, J. R. (2019). The Intersection of Cyberstalking, Gender and Capable Guardianship. Doctoral Dissertation, Arkansas State University.

Gikas, C. (2010). A General Comparison of FISMA, HIPAA, ISO 27000 and PCI-DSS Standards. *Information Security Journal: A Global Perspective, 19*(3), 132-141.

Goode, P. (2020). The Effect of Bandura's Self-Efficacy Concepts to Improve Diabetes Self-Management Practices. *Journal of Kidney Care*, *5*(2), 58-61.

Grønhøj, A., Bech-Larsen, T., Chan, K. and Tsang, L. (2012). A TPB Study of Adolescents' Intentions for Healthy Eating Consumption. In *Child and Teen Consumption 5th International Conference*.

Godlove, T. (2012). Examination of the Factors that Influence Teleworkers' Willingness to Comply with Information Security Guidelines. *Information Security Journal: A Global Perspective*, *21*(4), 216-229.

Goel, R., Kumar, A., and Haddow, J. (2020). PRISM: a strategic decision framework for cybersecurity risk assessment. *Information and Computer Security*.

Goodhue, D. L. and Straub, D. W. (1991). Security Concerns of System Users: A Study of Perceptions of the Adequacy of Security. *Information and Management*, *20*(1), 13-27.

Goosen, L., and Soga, H. A. (2019, September). Information Systems Architecture and Governance of Enterprise Information Technology at a Regulatory Institution. In *International Conference on Information Systems Architecture and Technology* (pp. 141-150). Springer, Cham.

Good, V. R. (2019). Identity Theft and the Internet. *Doctoral Dissertation*, Utica College.

Grinter, R., and Eldridge, M. (2003, April). Wan2tlk?: Everyday Text Messaging. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 441-448). ACM.

Guan, B. and Hsu, C. (2020). The Role of Abusive Supervision and Organisational Commitment on Employees' Information Security Policy Noncompliance Intention. *Internet Research. Ahead-Of-Print.* 10.1108/INTR-06-2019-0260.

Guhr, N., Lebek, B., and Breitner, M. H. (2019). The Impact of Leadership on Employees' Intended Information Security Behaviour: An Examination of the Full-Range Leadership Theory. *Information Systems Journal*, *29*(2), 340-362.

Günbayi, I., and Sorm, S. (2018). Social Paradigms in Guiding Social Research Design: The Functional, Interpretive, Radical Humanist and Radical Structural Paradigms. *Online Submission*, *9*(2), 57-76.

Gundu, T. and Flowerday, S. V. (2013). Ignorance to Awareness: Towards an Information Security Awareness Process. *SAIEE Africa Research Journal*, *104*(2), 69-79.

Gunkel, D. J. (2018). *Hacking Cyberspace*. Routledge.

Guo, K. H. and Yuan, Y. (2012). The Effects of Multilevel Sanctions on Information Security Violations: A Mediating Model. *Information and Management*, *49*(6), 320-326.

Guobin, H., and Lin, Z. (2015). Big Data Information Security Risks and Coping Strategies. *Research on Library Science*, (13), 5.

Hagen, J. M. (2009). The Human Factor Behind the Security Perimeter. Evaluating the Effectiveness of Organisational Information Security Measures and Employees' Contributions to Security. *Oslo: University of Oslo*.

Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2010). Multivariate Data Analysis: International version. *New Jersey, Pearson*.

Hair Jr, J. F., Hult, G. T. M., Ringle, C., and Sarstedt, M. (2016). *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*. Sage Publications.

Hall, A., Turner, L. and Kilpatrick, S. (2019). Using the Theory of Planned Behaviour Framework to understand Tasmanian dairy farmer engagement with extension activities to inform future delivery. *The Journal of Agricultural Education and Extension*, *25*(3), 195-210.

Harrison, J. A., Mullen, P. D. and Green, L. W. (1992). A Meta-Analysis of Studies of the Health Belief Model with Adults. *Health Education Research*, *7*(1), 107-116.

Hassan, A. B., Lass, F. D. and Makinde, J. (2012). Cybercrime in Nigeria: Causes, Effects and the Way Out. *ARPN Journal of Science and Technology*, *2*(7), 626-631.

Hassandoust, F. and Techatassanasoontorn, A. A. (2020). Understanding Users' Information Security Awareness and Intentions: A Full Nomology of Protection Motivation Theory. In *Cyber Influence and Cognitive Threats* (pp. 129-143). Academic Press.

Hazari, S., Hargrave, W. and Clenney, B. (2008). An Empirical Investigation of Factors Influencing Information Security Behavior. *Journal of Information Privacy and Security*, *4*(4), 3-20.

Hemphill, T. A., and Longstreet, P. (2016). Financial Data Breaches in the US Retail Economy: Restoring Confidence in Information Technology Security Standards. *Technology in Society*, *44*, 30-38.

Heo, J. and Ahn, S. (2020). Effects of Biased Awareness of Security Policies on Security Compliance Behavior. *The Journal of Korean Association of Computer Education*, *23*(1), 63-75.

Herath, T. and Rao, H. R. (2009). Encouraging Information Security Behaviours in Organisations: Role of Penalties, Pressures and Perceived Effectiveness. *Decision Support Systems*, *47*(2), 154-165.

Herath, T., Chen, R., Wang, J., Banjara, K., Wilbur, J. and Rao, R. H. (2014). Security Services as Coping Mechanism: An Investigation into User Intention to Adopt an Email Authentication, *Info Systems Journal*, 61-64. doi:10.1111/j.1365-2575.2012. 00420.x

Héroux, S., Fortin, A., and Goupil, C. (2020). Adherence to Expense Report Approval Control: An Application of the Theory of Planned Behavior. *Journal of Applied Accounting Research* , Vol. 21 No. 3, pp. 397-413.

Hewitt, B., and White, G. L. (2020). Optimistic Bias and Exposure Affect Security Incidents On Home Computer. *Journal of Computer Information Systems*, 1-11.

Hinduja, S. (2007). Computer Crime Investigations in the United States: Leveraging Knowledge from the Past to Address the Future. *International Journal of Cyber Criminology, 1*(1), 1-26.

Hirose, A. S., Arakaki, R., Mittelsdorf, A. W., and Ruggiero, W. V. (2019). *U.S. Patent Application No. 16/071,652*, available at https://patentimages.storage.googleapis.com/fe/7e/21/63dc02262fde7c/US20190034661A1.pdf.

Holt, T. J. (2020). Computer Hacking and the Hacker Subculture. *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, 725-742.

Hong, J. (2012). The Current State of Phishing Attacks. *Communications of the ACM*, *55*(1), 74-81.

Hong, H. L. (2013). Feasibility Study on Incorporating IEC/ISOISO/IEC ISO/IEC 27001. Information Security Management System (ISMS) Standard in IT Services Environment. *Postgraduate Thesis.* Universiti Teknologi Malaysia.

Hong, Y. and Furnell, S. (2019, June). Organisational Formalization and Employee Information Security Behavioral Intentions Based on an Extended TPB model. In *2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)* (pp. 1-4). IEEE

Hooper, V., and Blunt, C. (2020). Factors Influencing the Information Security Behaviour of IT Employees. *Behaviour and Information Technology*, *39*(8), 862-874.

Hovav, A. and D'Arcy, J. (2012). Applying an Extended Model of Deterrence Across Cultures: An Investigation of Information Systems Misuse in the US and South Korea. *Information and Management*, *49*(2), 99-110.

Hovav, A. and D'Arcy, J. (2003). The Impact of Denial-Of-Service Attack Announcements on the Market Value of Firms. *Risk Management and Insurance Review*, *6*(2), 97-121.

Hu, Q., Dinev, T., Hart, P., and Cooke, D. (2012). Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organisational Culture. *Decision Sciences*, *43*(4), 615-660.

Humaidi, N., and Balakrishnan, V. (2015). Leadership Styles and Information Security Compliance Behavior: The Mediator Effect of Information Security Awareness. *International Journal of Information and Education Technology*, *5*(4), 311.

Hussain, M., Nadeem, M. W., Iqbal, S., Mehrban, S., Fatima, S. N., Hakeem, O. and Mustafa, G. (2019). Security and Privacy in FinTech: A Policy Enforcement Framework. In *FinTech as a Disruptive Technology for Financial Institutions* (pp. 81-97). IGI Global.

Hu, Q., Xu, Z., Dinev, T. and Ling, H. (2011). Does Deterrence Work in Reducing Information Security Policy Abuse by Employees? *Commun. ACM*, *54*(6), 54-60.

Huang, D., Rau, P.P. and Salvendy, G. (2007). A Survey of Factors Influencing People's Perception of Information Security. In J. Jacko (Ed.). *Human-Computer Interaction, Part IV* (pp. 906-915). Heidelberg: Springer.

Huang, D.-L., Rau, P.-L. P. and Salvendy, G. (2010). Perception of Information Security. *Behaviour and Information Technology*, *29*(3), 221-232.

Humphreys, E. (2008). Information Security Management Standards: Compliance, Governance and Risk Management. *Information security technical report*, *13*(4), 247-255.

Huntsman (2015). Fraud Prevention and I.T. Security: Using Huntsman to Align Fraud prevention and IT Security. *A White Paper Report of Huntsman.*

Hwang, I., and Cha, O. (2018). Examining Technostress Creators and Role Stress As Potential Threats to Employees' Information Security Compliance. *Computers in Human Behavior*, *81*, 282-293.

Ibikunle, F., and Eweniyi, O. (2013). Approach to Cyber Security Issues in Nigeria: Challenges and Solutions. *International Journal of Cognitive Research in Science, Engineering and Education, (IJCRSEE, 1 (1). Retrieved from* http://ijcrsee.com/index.php/ijcrsee/article/view/11/114 on 28th September, 2016.

Ifinedo, P. (2012). Understanding Information Systems Security Policy Compliance: An Integration of the Theory of Planned Behaviour and the Protection Motivation Theory. *Computers and Security*, *31*(1), 83-95. doi: 10.1016/j.cose.2011.10.007

Ifinedo, P. (2013). Relationships Between Relevant Contextual Influences and Information Security Threats and Controls in Global Financial Services Industry. *Journal of Computing and Information Technology*, *21*(4), 235-246.

Ifinedo, P. (2014). Information Systems Security Policy Compliance: An Empirical Study of The Effects of Socialisation, Influence and Cognition. *Information and Management*, *51*(1), 69-79.

Ikpefan, O. A. (2006). *Growth of Bank Frauds and the Impact on the Nigerian Banking Industry,* Research Report for Covenant University, Ota, Ogun State.

Islam, S. (2020). Enhanced Information System Security in Internet Banking and Manufacturing. *International Journal of Engineering Materials and Manufacture*, *5*(2), 62-67.

Itai, Y. and Onwubiko, E. (2019). Combating Insider Fraud in Financial Institutions/Impact. *International Journal of Management and Information Technology*, *14*, 3351-3358.

Iriqat, Y. M. and Molok, N. N. A. (2019, April). Information Security Policy Perceived Compliance Among Staff in Palestine Universities: An Empirical Pilot Study. In *2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT)* (pp. 580-585). IEEE.

ITP (2010). UAE Bank Targeted in Major Phishing Attacks. Available at: http://www.itp.netl579059-uae-banktargeted-in-major-phishing-attack

Jain, P. (2020). Likert Scale Development–Construction and Evaluation of Financial Behavior Scale (FBS). *Studies in Indian Place Names*, *40*(26), 179-186.

Jalali, M., Bruckes, M., Westmattelmann, D. and Schewe, G. (2019). Why Employees (Still) Click on Phishing Links: An Investigation in Hospitals. *Journal of Medical Internet Research.* 22(1). *Available at https://www.jmir.org/2020/1/e16775/*

Jassal, R. K., and Sehgal, R. K. (2013). Study of Online Banking Security Mechanism in India: Take ICICI Bank as an Example. *IOSR Journal of Computer Engineering (IOSR-*

JCE), *13*(1), 114-121.

Jaynes, C. M., and Loughran, T. A. (2020). How Offender Decision-Making Can Inform Policing: A Focus on the Perceived Certainty of Apprehension. In *Science Informed Policing* (pp. 3-18). Springer, Cham.

Jegede, A. E. (2014). Cyber Fraud, Global Trade and Youth Crime Burden: Nigerian Experience, *Afro Asian Journal of Social Sciences*, 5 (4), 1-21.

Jeno, L. M., Vandvik, V., Eliassen, S. and Grytnes, J. A. (2019). Testing the Novelty Effect of

an m-learning Tool on Internalization and Achievement: A Self-Determination Theory Approach. *Computers and Education*, *128*, 398-413.

Jiang, S., Dong, L., and Jiang, C. (2020). Examining the Link between Economic Strain and Adolescent Social Behavior: Roles of Social Bonds and Empathy. *Journal of Adolescence*, *84*, 1-10.

John, O. P., Naumann, L. P. and Soto, C. J. (2008). Paradigm Shift to the Integrative Big Five Trait Taxonomy. *Handbook of Personality: Theory and Research*, *3*(2), 114-158.

Johnston, A. C. and Warkentin, M. (2010). Fear Appeals and Information Security Behaviours: An Empirical Study. *MIS Quarterly*, 549-566.

Jones, R. and Pendlebury, M. (2000). *Public Sector Accounting.* 5th Edition. Financial Times/Division of Pearson Education.

Jusuf, Z., Arief, A. and Jamil, M. (2019). Audit Teknologi Informasi Untuk Evaluasi Manajemen Teknologi Informasi Menggunakan COBIT 5 dan IT Security (Studi Kasus: Dishubkominfo Provinsi Maluku Utara). *JIKO (Jurnal Informatika dan Komputer)*, *1*(1), 49-56.

Kadir, H. A., Rahmani, N. and Masinaei, R. (2011). Impacts of Service Quality on Customer Satisfaction: Study of Online Banking and ATM Services in Malaysia. *International Journal of Trade, Economics and Finance*, *2*(1), 1.

Kai, T. A. N. G. (2020). Risk Analysis of Industrial Internet Identity System. *Zte Communications*, *18*(1).

Kajava, J. and Siponen, M. T. (2002). IT Security Awareness - Issues for Industry. *European Intensive Programme on Information and Communication Technologies Security*. Available @

https://www.researchgate.net/publication/267794563_IT_Security_Awareness_-Issues_for_Industry/citation/download

Kamatchi, A., and Modi, C. (2016). An Efficient Security Framework to Detect Intrusions at Virtual Network Layer of Cloud Computing. In *Proceedings of the 19th Conference on Innovations in Clouds, Internet and Networks (ICIN).* March 1-3, 2016, Paris.

Kandasamy, I., Kandasamy, W. V., Obbineni, J. M., and Smarandache, F. (2020). Indeterminate Likert Scale: Feedback Based on Neutrosophy, Its Distance Measures and Clustering Algorithm. *Soft Computing*, *24*(10), 7459-7468.

Karjalainen, M., Siponen, M., Puhakainen, P., and Sarker, S. (2020). Universal and Culture-Dependent Employee Compliance of Information Systems Security Procedures. *Journal of Global Information Technology Management*, *23*(1), 5-24.

Kaya, S. Ş., Çavdaroğlu, B. and Şensoy, K. S. (2020). Detection of Click Spamming in Mobile Advertising. In *Advances in Operational Research in the Balkans* (pp. 251-263). Springer, Cham.

Kaymaz, K. (2020). The Analysis of the Relations among Normative Beliefs, Self-Efficacy and Intention to Comply Within the Frame of Information Security Policies. *Is, Guc: The Journal of Industrial Relations and Human Resources*, *22*(1) 64-91.

Kayisire, D. and Wei, J. (2015). ICT Adoption and Usage in Africa: Towards an Efficiency Assessment. *Journal of Information Technology for Development*. 22(4), 630-653. DOI: http://dx.doi.org/10.1080/02681102.2015.1081862

Kaymaz, k. (2020). The Analysis of the Relations Among Normative Beliefs, Self-Efficacy and Intention to Comply within the Frame of Information Security Policies. *The Journal of Industrial Relations and Human Resources*, *22*(1), 1-20

Karabacak, B., Yildirim, S. O., and Baykal, N. (2016). A vulnerability-driven cyber security maturity model for measuring national critical infrastructure protection preparedness. *International Journal of Critical Infrastructure Protection*, *15*, 47-59.

Kayode, A. B., Arome, G. J., Tolulope, A. and Ajoke, A. O. (2016). Cost-Benefit Analysis of Cyber-Security Systems. In *Proceedings of the World Congress on Engineering and Computer Science.*

Kearney, W. D. and Kruger, H. A. (2014). Considering the Influence of Human Trust in Practical Social Engineering Exercises. In *2014 Information Security for South Africa* (pp. 1-6). IEEE.

Kida, M. I. and Goyal, A. and Mbaniso, J. (2018). Empirical Study of the Challenges of Cashless Banking System in Nigeria with respect to Availability and Reliability of Cashless Banking Channels. *International Journal of Research in Engineering, IT and Social Sciences,* 8(8), 7-16

Kim, D., Chun, H. and Lee, H. (2014). Determining the Factors that Influence College Students' Adoption of Smartphones. *Journal of the Association for Information Science and Technology*, *65*(3), 578-588

Kim, H. L., Choi, H. S. and Han, J. (2019). Leader Power and Employees' Information Security Policy Compliance. *Security Journal*, 1-19.

Kim, M., and Park, S. O. (2013). Trust Management on User Behavioral Patterns for A Mobile Cloud Computing. *Cluster Computing*, *16*(4), 725-731.

Koohang, A., Nowak, A., Paliszkiewicz, J. and Nord, J. H. (2020). Information Security Policy Compliance: Leadership, Trust, Role Values, and Awareness. *Journal of Computer Information Systems*, *60*(1), 1-8.

Koranteng, F. N., Apau, R., Opoku-Ware, J. and Ekpezu, A. O. (2020). Evaluating the Effectiveness of Deterrence Theory in Information Security Compliance: New Insights from a Developing Country. In *Modern Theories and Practices for Cyber Ethics and Security Compliance* (pp. 140-151). IGI Global.

Kraemer, S., Carayon, P. and Clem, J. (2009). Human and Organisational Factors in Computer and Information Security: Pathways to Vulnerabilities. *Computers and Security*, *28*(7), 509-520.

Kreicberga, L. (2010). Internal Threat to Information Security: Countermeasures and Human Factor Within SME. *Postgraduate Thesis.* Luleå University of Technology.

Krejcie, R. V. and Morgan, D. W. (1970). Determining Sample Size for Research Activities. *Educational and Psychological Measurement*, 30(3), pp. 607-610.

Kreuter, M. W. and Strecher, V. J. (1995). Changing Inaccurate Perceptions of Health Risk: Results from a Randomized Trial. *Health Psychology*, *14* (1), 56. doi: 10.1037/0278-6133.14.1.56

Kumaraguru, P., Rhee, Y., Acquisti, A., Cranor, L. F., Hong, J. and Nunge, E. (2007). Protecting People from Phishing: The Design and Evaluation of an Embedded Training Email System. In *Proceedings of the SIGCHI conference on Human factors in Computing Systems* (pp. 905-914). ACM.

Lacey, T. A. and Wright, B. (2009). Employment Outlook: 2008-18 - Occupational Employment

Projections to 2018. *Monthly Lab. Rev.*, *132*, 82.

Lacohée, H., Phippen, A. D. and Furnell, S. M. (2006). Risk and Restitution: Assessing How Users Establish Online Trust. *Computers and Security*, *25*(7), 486-493.

Lacy, D. and Niou, E. M. (2004). A Theory of Economic Sanctions and Issue Linkage: The Roles of Preferences, Information, and Threats. *The Journal of Politics*, *66*(1), 25-42.

Lakshman, M., Sinha, L., Biswas, M., Charles, M. and Arora, N. K. (2000). Quantitative Vs Qualitative Research Methods. *The Indian Journal of Pediatrics*, *67*(5), 369-377. doi:10.1007/BF02820690

Laura, A. (1995). Cybercrime and National Security: The Role of the Penal and Procedural Law. *Nigeria Institute of Advanced Legal Studies.*

Lazarus, S., and Okolorie, G. U. (2019). The Bifurcation of the Nigerian Cybercriminals: Narratives of the Economic and Financial Crimes Commission (EFCC) Agents. *Telematics and Informatics*, *40*, 14-26.

Leach, J. (2003). Improving User Security Behaviour. *Computers and Security*, *22*(8), 685-692.

Lee, N. M. (2018). Fake News, Phishing, and Fraud: A Call for Research on Digital Media Literacy Education Beyond the Classroom. *Communication Education*, *67*(4), 460-466.

Lee, S. M., Lee, S.-G. and Yoo, S. (2004). An Integrative Model of Computer Abuse Based on Social Control and General Deterrence Theories. *Information and Management, 41*(6), 707-718.

Lee, C., Lee, C. C. and Kim, S. (2016). Understanding Information Security Stress: Focusing on the Type of Information Security Compliance Activity. *Computers and Security*, *59*, 60-70.

Leukfeldt, E. R., and Kleemans, E. E. (2019). 5 Cybercrime, Money Mules and Situational Crime Prevention. *Criminal Networks and Law Enforcement: Global Perspectives On Illegal*
Enterprise, 13.

Logan, P. Y. (2020). Crafting an Undergraduate Information Security Emphasis within Information Technology. *Journal of Information Systems Education*, *13*(3), 3.

Longshore, D., Chang, E. and Messina, N. (2005). Self-Control and Social Bonds: A Combined Control Perspective on Juvenile Offending. *Journal of Quantitative Criminology*, *21*(4), 419-437.

Liang, H., Saraf, N., Hu, Q. and Xue, Y. (2007). Assimilation of Enterprise Systems: The Effect Of Institutional Pressures and the Mediating Role of Top Management. *MIS quarterly*, 59-87.

Lin, N., and Roberts, K. R. (2020). The Normative Beliefs that Form Individual Food Safety Behavioral Intention: A Qualitative Explanatory Study. *Food Control*, 110, 106966.

Liu, Y., Loi, R., and Ngo, H. Y. (2020). Linking Organisational Social Exchange To Intention To Leave: Does Normative Commitment Matter? *The International Journal of Human Resource Management*, *31*(13), 1663-1683.

Lippke, S. (2020). Self-Efficacy Theory. *Encyclopedia of Personality and Individual Differences*, 4722-4727.

Liu, C., Wang, N., and Liang, H. (2020). Motivating Information Security Policy Compliance: The Critical Role of Supervisor-Subordinate Guanxi and Organisational Commitment. *International Journal of Information Management*, *54*, 102152.

Locke, E., and Latham, G. P. (2019). Reply to Commentaries on "The Development of Goal Setting Theory: A Half Century Retrospective". *Motivation Science, 5*(2), 114–115. https://doi.org/10.1037/mot0000145

Longe, O., Ngwa, O., Wada, F., Mbarika, V. and Kvasny, L. (2009). Criminal Uses of Information and Communication Technologies in Sub-Saharan Africa: Trends, Concerns and Perspectives. *Journal of Information Technology Impact*, *9*(3), 155-172.

Lund, J. and Aaro, L. E. (2004). Accident Prevention. Presentation of a Model Placing Emphasis on Human, Structural and Cultural Factors. *Safety Science, 42*(4), 271-324.

Luthans, F., Youssef, C. M. and Avolio, B. J. (2007). Psychological Capital: Investing and Developing Positive Organisational Behavior. *Positive Organisational Behavior, 1*(2), 9-24.

Lowry, P. B. and Moody, G. D. (2015). Proposing the Control-Reactance Compliance Model (CRCM) to Explain Opposing Motivations to Comply with Organisational Information Security Policies. *Information Systems Journal*, *25*(5), 433-463.

Ma, Q. and Pearson, M. J. (2005). ISO 17799: "Best Practices" in Information Security Management? Communications of the Association for Information Systems, 15(2020), pp. 577-591.

Maçada, A. C. G. and Luciano, E. M. (2010). The influence of Human Factors on Vulnerability to Information Security Breaches. In *AMCIS* (p. 351).

Maleka, M. B. (2011). A Gender-Based Analysis of ICT Adoption and Usage in South Africa. *Postgraduate Thesis*. University of the Witwatersrand.

Malik, M. S. and Islam, U. (2019). Cybercrime: An Emerging Threat to the Banking Sector of Pakistan. *Journal of Financial Crime*, 26(1), pp. 50-60.

Malimage, K. (2019). Application of Underutilized Theories in Fraud Research: Suggestions for Future Research. *Journal of Forensic and Investigative Accounting*, *11*(1).

Malzahn, D., Birnbaum, Z., and Wright-Hamor, C. (2020, June). Automated Vulnerability Testing via Executable Attack Graphs. In *2020 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)* (pp. 1-10). IEEE.

Martens, M., and De Wolf, R. (2018). Measuring The Cost and Impact of Cybercrime In Belgium (BCC): *D3. 1.2 Risk Perception Monitor Report* (2nd Wave, 2017), *11*(2), 35.

Mathieson, K. (1991). Predicting User Intentions: Comparing the Technology Acceptance Model with the Theory of Planned Behavior. *Information Systems Research*, *2*(3), 173-191.

McDowell, J., and Novis, G. (2001). The Consequences of Money Laundering and Financial Crime. *Economic Perspectives*, *6*(2), 6-10.

McGuire, M., and Dowling, S. (2013). Cybercrime: Cyber-Enabled Crimes – Fraud and Theft, in a Review of the Evidence. *Research Report 77*. Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/248621/horr75-chap2.pdf, on 28th September, 2016.

McIlwraith, A. (2006). *Information Security and Employee Behaviour: How to Reduce Risk Through Employee Education, Training and Awareness.* Gower Publishing, Ltd.

Meade, C. S., Graff, F. S., Griffin, M. L. and Weiss, R. D. (2008). HIV Risk Behavior among Patients with Co-Occurring Bipolar And Substance Use Disorders: Associations with Mania and Drug Abuse. *Drug and Alcohol Dependence*, *92*(1-3), 296-300.

Meke, E. S. (2012). Urbanization and Cyber Crime in Nigeria: Causes and Consequences. *European Journal of Computer Science and Information Technology*, *3*(9), 1-11.

Mendell, R. L. (2004). *Investigating Computer Crime in the 21st Century*. 2nd Edition. Charles C. Thomas Pub Ltd

Merhi, M. I., and Midha, V. (2012). The Impact of Training and Social Norms On Information Security Compliance: *Thirty Third International Conference on Information Systems*, Orlando 2012.

Merhi, M. I. and Ahluwalia, P. (2019). Examining the Impact of Deterrence Factors and Norms on Resistance to Information Systems Security. *Computers in Human Behavior*, *92*, 37-46.

Metalidou, E., Marinagi, C., Trivellas, P., Eberhagen, N., Skourlas, C., and Giannakopoulos, G. (2014). The Human Factor of Information Security: Unintentional Damage Perspective. *Procedia-Social and Behavioral Sciences*, *147*, 424-428.

Mierzwa, S., and Scott, J. (2017). Cybersecurity in Non-Profit and Non-Governmental Organisations. *Institute for Critical Infrastructure Technology*. Available @ https://icitech.org/wp-content/uploads/2017/02/ICIT-Brif-Cybersecurity-and-NGOs.pdf

Milhorn, H. T. (2007). *Cybercrime: How to Avoid Becoming a Victim*. Universal-Publishers.

Miller, R. M., Hannikainen, I. A., and Cushman, F. A. (2014). Bad Actions or Bad Outcomes?

Differentiating Affective Contributions to the Moral Condemnation of Harm. *Emotion*, *14*(3), 573.

Mishra, A., Gupta, N., and Gupta, B. B. (2020). Security Threats and Recent Countermeasures in Cloud Computing. In *Modern Principles, Practices, and Algorithms for Cloud Security* (pp. 145-161). IGI Global.

MK, N., and Ramayah, T. (2019). The Impact of Security Factors Towards Internet Banking Usage Intention among Malaysians. *Global Business and Management Research, 11(2).*

Moody, G. D., Siponen, M. and Pahnila, S. (2018). Toward a Unified Model of Information Security Policy Compliance. *MIS Quarterly*, *42*(1).

Moore, W. and Frye, S. A. (2019). A Review of the HIPAA, Part 1: History, PHI, and Privacy and Security Rules. *Journal of Nuclear Medicine Technology*, jnmt-119.

Moore, J. F., and Labovitch, B. A. (2013). *U.S. Patent No. 8,347,088*. Washington, DC: U.S. Patent and Trademark Office.

Moses-Òkè, R. O. (2012). Cyber Capacity without Cyber Security: A Case Study of Nigeria's National Policy for Information Technology (NPFIT). *The Journal of Philosophy, Science and Law*, *12*(1), 1-14.

Moulton, R., and Coles, R. S. (2003). Applying Information Security Governance. *Computers and Security, 22*(7), 580-584.

Muller, S. R., and Lind, M. L. (2020). Factors in Information Assurance Professionals' Intentions to Adhere to Information Security Policies. *International Journal of Systems and Software Security and Protection (IJSSSP)*, *11*(1), 17-32.

Mutimukwe, C., Kolkowska, E., and Grönlund, Å. (2019). Information Privacy in E-Service: Effect of Organisational Privacy Assurances on Individual Privacy Concerns, Perceptions, Trust and Self-Disclosure Behavior. *Government Information Quarterly*, 101413.

Myler, E., and Broadbent, G. (2006). ISO/IEC 17799: Standard for Security. *Information Management, 40*(6), 43.

Mwashiuya, H. T., and Mbamba, U. O. (2020). Relationship of Information and Communication Technology Adoption on Microfinance Institutions Operational Performance and Access to Financial Services in TANZANIA. *International Journal of Information, Business and Management*, *12*(1), 214-237.

Nasir, A., Arshah, R. A., and Ab Hamid, M. R. (2020, March). Information Security Culture for Guiding Employee's Security Behaviour: A Pilot Study. In *2020 6th International Conference on Information Management (ICIM)* (pp. 205-209). IEEE.

National Institute of Standards Technology (2014). Framework for Improving Critical Infrastructure Cybersecurity. *National Institute of Standards and Technology Gaithersburg, MD.*

Neghina, D-E., and Scarlat, E. (2013). Managing Information Technology Security in the Context of Cyber Crime Trends, *International Journal of Computer Communications, 8* (1), 97-104.

Neuman, L. W. (2007). *Social Research Methods, 6/E*. Pearson Education India

Ngo, H. Q., Ashikhmin, A., Yang, H., Larsson, E. G., and Marzetta, T. L. (2017). Cell-free massive MIMO versus small cells. *IEEE Transactions on Wireless Communications*, *16*(3), 1834-1850.

Nguyen, Q. N. and Kim, D. J. (2017, January). Enforcing Information Security Protection: Risk Propensity and Self-Efficacy Perspectives. In *Proceedings of the 50th Hawaii International Conference on System Sciences***.**

Nigerian National Bureau of Statistics (2009). NBS/EFCC Business Survey on Crime and Corruption and Awareness of EFCC in Nigeria, 2007: Summary Report. Abuja: Available @ https://www.google.com/search?client=firefox-b-dandq=NBS%2FEFCC+Business+Survey+on+Crime+%26Corruption+and+Awareness+of+EFCC+in+Nigeria

Nigerian National Bureau of Statistics (2010). NBS/EFCC Business Survey on Crime and Corruption and Awareness of EFCC in Nigeria, 2007: *Statistical Report.* Abuja:

Nigeria Inter-Banks Settlement Systems (NIBSS) (2015). Available @ www.nibss-plc.com.ng Accessed November 16, 2019

Nikolakopoulos, T. (2009). *Evaluating the Human Factor in Information Security.* Postgraduate Thesis, University of Oslo (pp,1-65).

National Information Technology Development Agency. Nigeria, NITDA. Retrieved from http://www.nitda.gov.ng/index.php/it-statistics access 16.11.2019

Nawaya, J. J., Jemimah, N. and Oye, N. D. (2019). Designing a Biometric (Finger) Using Multispectral Imaging Biometric Authentication Measures for Enhancing ATM Security in Nigeria. *International Journal of Computer Science and Mobile Computing,* 8 (11) 38-47.

Nohlberg, M. and Kowalski, S. (2008). The Cycle of Deception: A Model of Social Engineering Attacks, defences and Victims. In *Second International Symposium on Human Aspects of Information Security and Assurance (HAISA 2008),* Plymouth, UK, 8-9, 1-11.

Nyawanga, J. O. (2015). *Meeting the Challenge of Cyber Threats in Emerging Electronic Transaction Technologies in Kenyan Banking Sector*. Postgraduate thesis University of Nairobi, Kenya.

Oberheide, J., Song, D., & Goodman, A. (2014). *U.S. Patent No. 8,893,251*. Washington, DC: U.S. Patent and Trademark Office, also available at https://patents.google.com/patent/US8893251B2/en.

Odior, E. S. and Banuso, F. B. (2012). Cashless Banking in Nigeria: Challenges, Benefits and Policy Implications. *European Scientific Journal, 8*(12), 289-316.

Ogbu, S.E., Idris, S. and Ijagbemi, A. B. (2011). Information and Communication Technology (ICT): A Veritable Tool for Tourism Development in Nigeria, *Information Technology for People-Centred Development* (ITePED), 2011, Nigeria Computer Society (NCS).

Ohki, E., Harada, Y., Kawaguchi, S., Shiozaki, T., and Kagaya, T. (2009, November). Information Security Governance Framework. In *Proceedings of the First ACM Workshop On Information Security Governance* (pp. 1-6).

Ogunsola, L. A. (2005). Information and Communication Technologies and the Effects of Globalization: Twenty-First Century "Digital Slavery" for Developing Countries – Myth or Reality? *Electronic Journal of Academic and Special Librarianship,* 6, 1-2.

Ogunniye, G. B. and Afolabi, O. M. (2014). A Hybrid Authentication Mechanism for Preventing Phishing Attacks On E-Banking Systems: The Nigeria Case Study. *International Journal of Emerging Technology and Advanced Engineering*, *4*(12), 628-635.

Ojeka, S. A. and Ikpefan, O. A. (2012). Electronic Commerce, Automation and Online Banking in Nigeria: Challenges and Benefits. *International Journal of Innovation in the Digital Economy (IJIDE)*, *3*(1), 11-26.

Ojeniyi, J. A. and Abdulhamid, S. M. (2019). Security Risk Analysis in Online Banking Transactions: Using Diamond Bank as a Case Study. *International Journal of Education and Management Engineering*, *9*(2), 1.

Okeshola, F. B. and Adeta, A. K. (2013). The Nature, Causes and Consequences of Cyber Crime in Tertiary Institutions in Zaria-Kaduna State, Nigeria. *American International Journal of Contemporary Research*, *3*(9), 98-114.

Oliver, R. L. (1980). A Cognitive Model of the Antecedents and Consequences of Satisfaction Decisions. *Journal of Marketing Research*, *17*(4), 460-469.

Olufunke, O. I., Kehinde, A. W., and Pius, G. J. (2010). Access and utilization of information and Communication Technology Amongst Lecturers and Students in South-West Nigeria Public Universities. *East Africa Journal of Educational Research and Policy*, *4*.

Olya, H. G., and Han, H. (2020). Antecedents of Space Traveller Behavioral Intention. *Journal of Travel Research*, *59*(3), 528-544.

Olusola, M., Samson, O., Semiu, A., & Yinka, A. (2013). Impact of Cyber Crimes on Nigerian Economy. *The International Journal of Engineering and Science (IJES)*, *12*(4), 45-51.

Onifade, A. B., Akinwande, K. A. and Shehu, H. (2019). Information Ethics: Islamic Perspectives on Privacy and Hacking. *Journal of Knowledge and Communication Management*, *9*(1), 29-44.

Onyesolu, M. O. and Ezeani, I. M. (2012). ATM Security Using Fingerprint Biometric Identifier:

An Investigative Study. *International Journal of Advanced Computer Science and Applications*, 3(4), 68-72.

Opoku-Ware, F. N. K. J. and Apau, R. (2020). Evaluating the Effectiveness of Deterrence Theory in Information Security Compliance. *Modern Theories and Practices for Cyber Ethics and Security Compliance*, 140.

Orji, U. J. (2019). Protecting Consumers from Cybercrime in the Banking and Financial Sector: An Analysis of the Legal Response in Nigeria. *Tilburg Law Review*, *24*(1).

Osasona, T. (2015). Time to Reform Nigeria's Cjustice System. *Journal of Law and Criminal Justice*, *3*(2), 73-79.

Oteng-Peprah, M., de Vries, N., and Acheampong, M. A. (2020). Households' Willingness to Adopt Greywater Treatment Technologies in A Developing Country–Exploring A Modified Theory of Planned Behaviour (TPB) Model Including Personal Norm. *Journal of Environmental Management*, *254*, 109807.

Owusu, G. M. Y., Bekoe, R. A., Addo-Yobo, A. A., & Otieku, J. (2020). Mobile Banking Adoption among the Ghanaian Youth. *Journal of African Business*, 1-22.

Pahnila, S., Siponen, M. and Mahmood, A. (2007, January). Employees' Behavior Towards IS Security Policy Compliance. In *2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07)* (pp. 156b-156b). IEEE.

Pahnila, S., Siponen, M., and Mahmood, A. (2007). Employees' behaviour towards IS security policy compliance. In *System sciences, 2007. HICSS 2007. 40Th annual Hawaii international conference* (pp. 156b-156b). IEEE.

Pallant, J., and Manual, S. S. (2010). *A Step by Step Guide to Data Analysis Using SPSS.* Berkshire UK: McGraw-Hill Education.

Pallant, J. (2011) *SPSS Survival Manual: A Step by Step Guide to Data Analysis Using SPSS for Windows.* Australia: Allen and Unwin.

Park, J. Y. (2013). The Study of Online Piracy Protection-Focusing on Punishment and Moral Obligation. *Journal of Digital Convergence*, *11*(1), 145-151.

Parkin, D. M. and Bray, F. (2009). Evaluation of Data Quality in The Cancer Registry: Principles and Methods Part II. Completeness. *European journal of cancer*, *45*(5), 756-764.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M. and Jerram, C. (2014). Determining Employee Awareness Using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers and Security*, *42*, 165-176.

Pathari, V., and M. Sonar, R. (2013). Deriving an Information Security Assurance Indicator at the Organisational Level. *Information Management and Computer Security*, *21*(5), 401-419.

Peffers, K., Tuunanen, T., Gengler, C. E., Rossi, M., Hui, W., Virtanen, V., and Bragge, J. (2020). Design Science Research Process: A Model for Producing and Presenting Information Systems Research. *arXiv preprint arXiv:2006.02763*.

Peterson, M. (2014). Identification of Behavioural Factors within Organisations that Can Improve Information Systems Security Compliance Master of Science university of Oregon state. Also available at: https://scholarsbank.uoregon.edu/xmlui/bitstream/handle/1794/19645/Peterson2014.pdf?sequence=1&isAllowe.

Pfleeger, S. L. and Caputo, D. D. (2012). Leveraging Behavioural Science to Mitigate Cyber Security Risk. *Computers and Security*, *31*(4), 597-611.

Pfleeger, S. L., Sasse, M. A. and Furnham, A. (2014). From Weakest Link to Security Hero: Transforming Staff Security Behavior. *Journal of Homeland Security and Emergency Management*, *11*(4), 489-510.

Pham, H., Brennan, L., and Richardson, J. (2017). Review of Behavioural Theories in Security Compliance and Research Challenge. In *The Proceedings of the Informing Science and Information Technology Education Conference, in Vietnam, Informing Science Institute, Santa Rosa, CA* (pp. 65-76).

Podsakoff, P. M., MacKenzie, S. B., Lee, J. Y. and Podsakoff, N. P. (2003). Common Method Biases in Behavioral Research: A Critical Review of the Literature and Recommended Remedies. *Journal of Applied Psychology*, *88*(5), 879.

Ponemon Institute (2013). The State of Advanced Persistent Threats. *Ponemon Research Report*, Available @

https://informationsecurity.report/Resources/Whitepapers/b92cfb99-1e2b-4c3d-9803-4720b7bb0d36_state-advanced-persistent-threats-pdf-6-w-1053.pdf

Quarshie, H. O. (2014). Using ICT to Fight Crime-A Case of Africa. *Journal of Emerging Trends in Computing and Information Sciences*, *5*(1), 21-24.

Raddatz, N. I., Marett, K., and Trinkle, B. S. (2020). The Impact of Awareness of Being Monitored on Computer Usage Policy Compliance: An agency View. *Journal of Information Systems*, *34*(1), 135-149.

Rasheed, H. (2014). Data and Infrastructure Security Auditing in Cloud Computing Environments. *International Journal of Information Management*, *34*(3), 364-368.

Rodrigues, K. L., Eves, A., Das Neves, C. P., Souto, B. K. and Dos Anjos, S. J. G. (2020). The Role of Optimistic Bias in Safe Food Handling Behaviours in the Food Service Sector. *Food Research International*, *130,* 108732.

Romanosky, S. (2016). Examining The Costs and Causes of Cyber Incidents. *Journal of Cybersecurity*, *2*(2), 121-135

Rosado, J. T., and Hernandez, A. A. (2020, February). An Empirical Examination of the Factors Influencing the Intention to Use Health Information System with Decision Support for Stroke Risk Assessment and Prediction. In *2020 16th IEEE International Colloquium on Signal Processing and Its Applications (CSPA) 14(*2), 278-283 IEEE.

Roth, A., and Rosenzweig, E. (2020). Advancing Empirical Science in Operations Management Research: A Clarion Call to Action. *Manufacturing and Service Operations Management*, *22*(1), 179-190.

Safa, N. S., Von Solms, R. and Furnell, S. (2016). Information Security Policy Compliance Model in Organisations. C*omputers and Security*, *56*, 70-82.

Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., and Herawan, T. (2015). Information Security Conscious Care Behaviour Formation in Organisations. *Computers and Security*, *53*, 65-78.

Safianu, O., Twum, F., and Hayfron-Acquah, J. B. (2016). Information System Security Threats and Vulnerabilities: Evaluating The Human Factor in Data Protection. *International Journal of Computer Applications*, *975*, 8887.

Sarantakos, S. (2013). *Social Research*. 4th Edition. Hampshire: Palgrave Macmillan.

Saulawa, M. A. A. and Abubakar, M. K. (2014). Cybercrime in Nigeria: An Overview of Cybercrime Act 2013. *JL Pol'y and Globalization*, *32*, 23-33.

Saunders, M. N., and Bezzina, F. (2015). Reflections on Conceptions of Research Methodology Among Management Academics. *European Management Journal*, *33*(5), 297-304.

Saunders, M. N. (2012). Choosing research participants. *Qualitative organisational research: Core methods and current challenges*, 35-52.

Saxton, G. D., and Neely, D. G. (2019). The Relationship Between Sarbanes–Oxley Policies and Donor Advisories in Nonprofit Organisations. *Journal of Business Ethics*, *158*(2), 333-351.

Sattarova Feruza, Y. and Kim, T. H. (2007). IT Security Review: Privacy, Protection, Access Control, Assurance and System Security. *International Journal of Multimedia and Ubiquitous Engineering*, *2*(2), 17-32.

Schunk, D. H., and Dibenedetto, M. K. (2020). Motivation and Social Cognitive Theory. *Contemporary Educational Psychology*, *60*, 101832.

Schuurman, B. (2020). Research On Terrorism, 2007–2016: A Review of Data, Methods, and Authorship. *Terrorism and Political Violence*, *32*(5), 1011-1026.

Selamat, M. H. and Babatunde, D. A. (2014). Mediating Effect of Information Security Culture on the Relationship Between Information Security Activities and Organisational Performance in the Nigerian Banking Setting. *International Journal of Business and Management*, *9*(7), 33.

Sekaran, U. (2009). *Research Methods for Business: A Skill Building Approach.* 5th Edition, John Wiley and Sons Ltd.: United Kingdom

Setiawan, D. A. (2019). Perkembangan Modus Operandi Kejahatan Skimming Dalam Pembobolan Mesin Atm Bank Sebagai Bentuk Kejahatan Dunia Maya (Cybercrime). Era Hukum-Jurnal Ilmiah Ilmu Hukum, 16(2).

Sharma, S., and Warkentin, M. (2019). Do I Really Belong? Impact of Employment Status on Information Security Policy Compliance. *Computers and Security*, *87*, 101397.

Sheikhpour, R., and Modiri, N. (2012). An Approach to Map Cobit Processes to ISO/IEC ISO/IEC ISO/IEC 27001 Information Security Management Controls. *International Journal of Security and its Applications*, *6*(2), 13-28.

Singh, R., Pandiya, B., Upadhyay, C. K., and Singh, M. K. (2020). It-Governance Framework Considering Service Quality and Information Security in Banks in India. *International Journal of Human Capital and Information Technology Professionals (IJHCITP)*, *11*(1), 64-91.

Sinha, P., Kumar Rai, A., and Bhushan, B. (2019, July). Information Security Threats and Attacks with Conceivable Counteraction. In *2019 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT)* (Vol. 1, Pp. 1208-1213). IEEE.

Smith, E. P. and Iacobelli, D. V. (2013). Analyzing Local and Global Fraud. *The CPA Journal*, *83*(6), 9.

Soodan, V., and Rana, A. (2020). Modeling Customers' Intention to Use E-Wallet in A Developing Nation: Extending UTAUT2 with Security, Privacy and Savings. *Journal of Electronic Commerce in Organisations (JECO)*, *18*(1), 89-114.

Soomro, Z. A., Shah, M. H., and Ahmed, J. (2016). Information Security Management Needs More Holistic Approach: A Literature Review. *International Journal of Information Management*, *36*(2), 215-225.

Spengler, B., Hofer, J., and Busch, H. (2020). Somebody Hit the Button! The Implicit Power Motive and The Frequency of Verbal Persuasion Behavior in Children. *Motivation and Emotion*, 1-9.

Su, K. (2016). Managing Mobile Device Usage Agreement. Retrieved From Www.Snowsoftware.Com/Int/Blog/2016/10/06/Managing-Mobile-Device-Usageagreements.

Susanto, H., and Almunawar, M. N. (2018). *Information Security Management Systems: A Novel Framework and Software as a Tool for Compliance with Information Security Standard*. Apple Academic Press.

Sharma, S. K. and Sharma, M. (2019). Examining The Role of Trust and Quality Dimensions in the Actual Usage of Mobile Banking Services: An Empirical Investigation. *International Journal of Information Management*, *44*, 65-75.

Sharot, T. (2011). The Optimism Bias. *Current Biology*, *21*(23), R941-R945.

Shaw, R. S., Chen, C. C., Harris, A. L., and Huang, H. J. (2009). The Impact of Information Richness on Information Security Awareness Training Effectiveness. *Computers and Education*, *52*(1), 92-100.

Siddique, M. I., and Rehman, S. (2011). Impact of Electronic Crime in Indian Banking Sector: an overview. *International Journal of Business and Information Technology*, *1*(2), 159-164.

Silverman, D. (2019). *Interpreting Qualitative Data*. SAGE Publications Limited.

Siponen, M., Mahmood, M. A., and Pahnila, S. (2014). Employees' Adherence to Information Security Policies: An Exploratory Field Study. *Information and Management*, *51*(2), 217-224.

Sims, R. L. (2012). Ethical Rule Breaking by Employees: A Test of Social Bonding Theory. *Journal of Business Ethics*, *40*(2), 101-109.

Smith, T. D., Eiting, T. P., and Bhatnagar, K. P. (2012). A Quantitative Study of Olfactory, Non-

Olfactory, and Vomeronasal Epithelia in the Nasal Fossa of the Bat Megaderma Lyra. *Journal of Mammalian Evolution*, *19*(1), 27-41.

Smith, A. M. (2012). Research Methodology: A Step-By-Step Guide for Beginners. *Nurse Education in Practice*, *12*(3),25.

Sniehotta, F. (2009). An Experimental Test of the Theory of Planned Behavior. *Applied Psychology: Health and Well-Being*, *1*(2), 257-270.

Sommestad, T., Karlzén, H., and Hallberg, J. (2015). The Sufficiency of the Theory of Planned Behavior for Explaining Information Security Policy Compliance. *Information and Computer Security*, *23*(2), 200-217.

Spulbar, C., and Birau, R. (2020). The Effects of Cybercrime on the Banking Sector in ASEAN. In *Financial Technology and Disruptive Innovation in ASEAN* (130-148).

Stamland, F. A. (2004). *Is BS 7799 worth the effort?* (Master's thesis).

Standard, A. (2015). ISO/IEC27002. In I*nformation Technology-Security Techniques-Code of Practice for Information Security Controls (AS ISO/IEC 27002: 2015)*.

Stamp, M. (2011). *Information Security: Principles and Practice*. John Wiley and Sons. Available at https://books.google.com.ng/books?hl=en&lr=&id=UW3SS9P9hdEC&oi=fnd&pg=PA12&dq=Stamp,+M.+(2011).+Information+Security:+Principles+and+Practice.+John+Wiley+and+Sons.&ots=0XK8Bdx8UF&sig=HykeeAsXyke0fMPA0ikgdbvj7-c&redir_esc=y#v=onepage&q=Stamp%2C%20M.%20(2011).%20Information%20Security%3A%20Principles%20and%20Practice.%20John%20Wiley%20and%20Sons.&f=false.

Sunday, I-O., and Bamidele, E. H. (2014). Financial Crime and its Implications on Banks Performance in Nigeria: A General Appraisal. *International Journal of Sciences: Basic and Applied Research*, *13*(2), 317-328.

Susanto, H., Almunawar, M. N., and Tuan, Y. C. (2011). Information Security Management System Standards: A Comparative Study of the Big Five. *International Journal of Electrical Computer Sciences IJECSIJENS*, *11*(5), 23-29.

Thakkar, A., Badsha, S., and Sengupta, S. (2020, January). Game Theoretic Approach Applied in Cybersecurity Information Exchange Framework. In *2020 IEEE 17th Annual Consumer Communications and Networking Conference (CCNC)* (pp. 1-7). IEEE.

Thang, N. C., Mai, l. H., Chi, N. T. K., and Kien, V. T. (2019). Factors Affecting the Intention to Use of Internet Banking of Customers in Vietnam's Commercial Banks in Industrial Revolution Context 4.0. *вестник челябинского государственного университета*, (7 (429).

Thomson, K.-L., and Von Solms, R. (2005). Information Security Obedience: A Definition. *Computers and Security*, *24*(1), 69-75.

Tinnilä, M. (2012). Impact of Future Trends on Banking Services. *Journal of Internet Banking and Commerce*, *17*(2), 1.

Tsohou, A., Karyda, M., Kokolakis, S., and Kiountouzis, E. (2015). Managing the Introduction of Information Security Awareness Programmes in Organisations. *European Journal of Information Systems*, *24*(1), 38-58.

Tyler, T. R., and Blader, S. L. (2005). Can businesses effectively regulate employee conduct? The antecedents of rule following in work settings. *Academy of Management Journal*, *48*(6), 1143-1158.

Ula, M., Ismail, Z., and Sidek, Z. M. (2011). A Framework for the Governance of Information Security in Banking Systems. *Journal of Information Assurance and Cyber Security*, 1-12.

Umejiaku, N. O., and Anyaegbu, M. I. (2016). Legal Framework for The Enforcement of Cyber Law and Cyber Ethics in Nigeria. *International Journal of Computer and Technology*, *15*, 7130-7139.

Usher, M., Tsetsos, K., Glickman, M., and Chater, N. (2019). Selective Integration: An Attentional Theory of Choice Biases and Adaptive Choice. *Current Directions in Psychological Science*, *28*(6), 552-559.

Van Bavel, R., Rodríguez-Priego, N., Vila, J., and Briggs, P. (2019). Using Protection Motivation Theory in the Design of Nudges to Improve Online Security behavior. *International Journal of Human-Computer Studies*, *123*, 29-39.

Van Ginkel, J. R., Linting, M., Rippe, R. C., and Van Der Voort, A. (2020). Rebutting Existing Misconceptions About Multiple Imputation as A Method for Handling Missing Data. *Journal of Personality Assessment*, *102*(3), 297-308.

Van Kessel, P., and Allah. K. (2013). Insights on Governance, Risk, and Compliance. Under Cyber Attack EY's Global Information Security Survey. Retrieved from http://www.ey.com/Publication/vwLUAssets/EY__2013_Global_Information_Security_Survey/$FILE/EY-GIS6S-Under-cyber-attack.pdf, on 28th September, 2016

Vance, A., Siponen, M. T., and Straub, D. W. (2020). Effects of Sanctions, Moral Beliefs, and Neutralization on Information Security Policy Violations Across Cultures. *Information and Management*, *57*(4), 103212.

Vance, A., and Siponen, M. T. (2012). IS Security Policy Violations: A Rational Choice Perspective. *Journal of Organisational and End User Computing (JOEUC)*, *24*(1), 21-41.

Vance, A. T. (2012). *Real David Harum*. Hardpress Publishing.

Vateva-Gurova, T., Luna, J., Pellegrino, G., and Suri, N. (2014). Towards A Framework for Assessing the Feasibility of Side-Channel Attacks in Virtualized Environments. Paper Presented at The 11th International Conference On Security and Cryptography (Secrypt): Vienna, Austria, August 2014.

Veltsos, J. R. (2012). An Analysis of Data Breach Notifications as Negative News. *Business Communication Quarterly*, *75*(2), 192-207.

Van Kessel, P., and Allan, K. (2013). Under Cyber-Attack. Ey's Global Information Security Survey 2013. *Ernst and Young*.

Verkoeyen, S., and Nepal, S. (2019). Threat and Coping Appraisal as Mediators of Adaptation Intentions in Place Attached and Activity Involved Scuba Divers. *Leisure Sciences*, 1-22.

Von Solms, R., and Van Niekerk, J. (2013). From Information Security to Cyber Security. C*omputers and Security*, *38*, 97-102.

Wada, F., and Odulaja, G. (2012). Electronic Banking and Cyber Crime in Nigeria - A Theoretical Policy Perspective on Causation. *Afr. J. Comput. ICT, 4*(2), 69-82.

Walliman, N. S. and Walliman N. (2011). *Research Methods: The Basics.* Taylor and Francis.

Walsh, J. L. (2019). Applying The Information–Motivation–Behavioral Skills Model to Understand Prep Intentions and Use Among Men Who Have Sex with Men. *Aids and Behavior*, *23*(7), 1904-1916.

Wang, E. S. T., and Chou, C. F. (2020). Norms, Consumer Social Responsibility and Fair Trade Product Purchase Intention. *International Journal of Retail and Distribution Management*.

Wang, J., Shan, Z., Gupta, M., and Rao, H. R. (2019). A Longitudinal Study of Unauthorized Access Attempts on Information Systems: The Role of Opportunity Contexts. *MIS Quarterly*, *43*(2).

Wei, Y. C., Wu, W. C., Lai, G. H., & Chu, Y. C. (2020). Privacy considered information security risk assessment model. *The Journal of Supercomputing*, *76*(3), 1468-1481.

Whitman, M., and Mattord, H. J. (2014). Information Security Governance for the Non-Security Business Executive Journal of Executive Education. 11(1).

Whitman, M. E., and Mattord, H. J. (2011). *Principles of Information Security*: Cengage Learning.

Wiafe, I., Koranteng, F.N., Wiafe, A., Obeng, E.N. and Yaokumah, W. (2020). The Role of Norms in Information Security Policy Compliance. *Information and Computer Security*, Vol. Ahead-of-Print No. Ahead-Of-Print. https://doi.org/10.1108/ICS-08-2019-0095.

Williams, A. S., Maharaj, M. S., and Ojo, A. I. (2019). Employee Behavioural Factors and Information Security Standard Compliance in Nigeria Banks. *International Journal of Computing and Digital Systems*, *8*(04), 387-396.

Williams, S.O. (2019). Accident Prevention Model for the Building Construction Industry. *Postgraduate Thesis*. Universiti Teknologi Malaysia.

Willison, R., and Warkentin, M. (2013). Beyond Deterrence: An Expanded View of Employee Computer Abuse. *MIS quarterly*, 1-20.

Wolden, M., Valverde, R., and Talla, M. (2015). The Effectiveness of COBIT 5 Information Security Framework for Reducing Cyber-Attacks on Supply Chain Management System. *Ifac-Papersonline*, 48(3), 1846-1852.

Wu, Y. C., Sun, R., and Wu, Y. J. (2020). Smart City Development in Taiwan: From the Perspective of the Information Security Policy. *Sustainability*, *12*(7), 2916.

Wu, A., Zhang, Y., Zheng, X., Guo, R., Zhao, Q., and Zheng, D. (2019). Efficient and Privacy-Preserving Traceable Attribute-Based Encryption in Blockchain. *Annals of Telecommunications*, 1-11.

Xiao, S., Warkentin, M., Walden, E., and Johnston, A. C. (2020). Do We Protect What We Own? A Proposed Neurophysiological Exploration of Workplace Information Protection Motivation. In *Information Systems and Neuroscience* (Pp. 101-109). Springer, Cham.

Yazdanmehr, A., Wang, J., and Yang, Z. (2020). Peers Matter: The Moderating Role of Social Influence On Information Security Policy Compliance. *Information Systems Journal* available at https://onlinelibrary.wiley.com/doi/epdf/10.1111/isj.12271.

Yazdanmehr, A. and Wang, J. (2016). Employees' Information Security Policy Compliance: A Norm Activation Perspective. *Decision Support Systems*, *92*, 36-46.

Yeh, Q.-J., and Chang, A. J.-T. (2007). Threats and countermeasures for information system security: A cross-industry study. *Information and Management*, *44*(5), 480-491.

Yoko, Z. G., Volk, K. L., Dochtermann, N. A., and Hamilton, J. A. (2020). The Importance of Quantitative Trait Differentiation in Restoration: Landscape Heterogeneity And Functional Traits Inform Seed Transfer Guidelines. *AOB Plants*, *12*(2), Plaa009.

Yoon, C., Hwang, J. W., and Kim, R. (2019). Exploring Factors That Influence Students' Behaviors in Information Security. *Journal of Information Systems Education*, *23*(4), 7.

Yuan, C. T., Nembhard, I. M., and Kane, G. C. (2020). The Influence of Peer Beliefs On Nurses' Use of New Health Information Technology: A Social Network Analysis. *Social Science and Medicine*, 113002.

Zajko, M. (2018). Security Against Surveillance: IT Security as Resistance to Pervasive Surveillance. *Surveillance and Society*, *16*(1), 39-52.

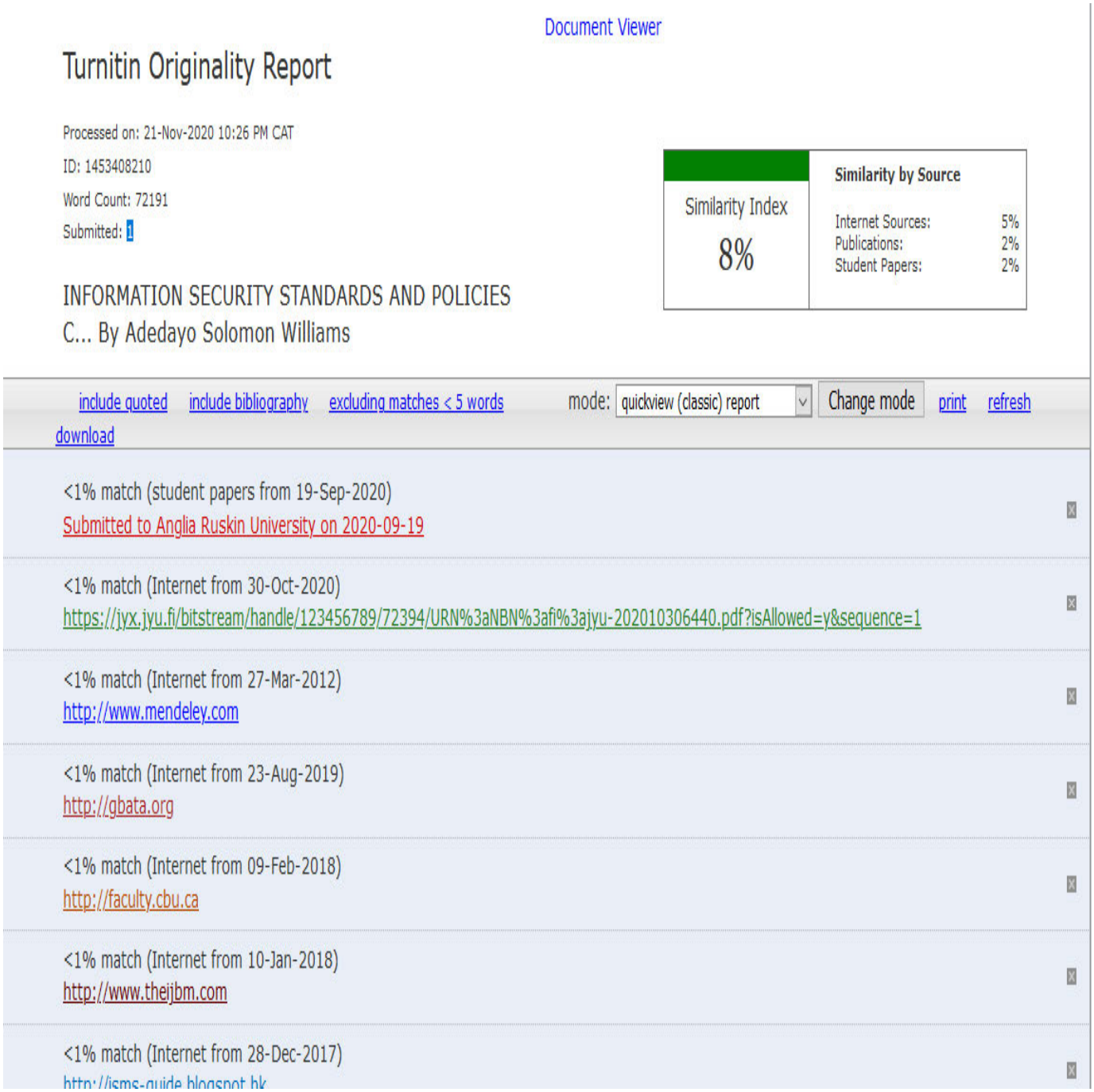
Zikmund-Fisher, B. J. (2019). Helping People Know Whether Measurements Have Good or Bad Implications: Increasing the Evaluability of Health and Science Data Communications. *Policy Insights from the Behavioral and Brain Sciences*, *6*(1), 29-37.

Zikmund, W. G., Babin, B. J., Carr, J. C., and Griffin, M. (2010). *Business Research Methods.* South-Western, Cengage Learning. Mason, OH.

Zikmund-Fisher, B. J. (2019). Helping People Know Whether Measurements Have Good or Bad Implications: Increasing the Evaluability of Health and Science Data Communications. *Policy Insights from the Behavioral and Brain Sciences*, *6*(1), 29-37.

Zohrabi, M. (2013). Mixed Method Research: Instruments, Validity, Reliability and Reporting Findings. *Theory and Practice in Language Studies*, 3, 254.

Appendix A: Originality Report



Document Viewer

Turnitin Originality Report

Processed on: 21-Nov-2020 10:26 PM CAT
ID: 1453408210
Word Count: 72191
Submitted: 1

INFORMATION SECURITY STANDARDS AND POLICIES
C... By Adedayo Solomon Williams

Similarity Index	Similarity by Source	
8%	Internet Sources:	5%
	Publications:	2%
	Student Papers:	2%

include quoted include bibliography excluding matches < 5 words mode: quickview (classic) report Change mode print refresh download

<1% match (student papers from 19-Sep-2020)
Submitted to Anglia Ruskin University on 2020-09-19

<1% match (Internet from 30-Oct-2020)
https://jyx.jyu.fi/bitstream/handle/123456789/72394/URN%3aNBN%3afi%3ajyu-202010306440.pdf?isAllowed=y&sequence=1

<1% match (Internet from 27-Mar-2012)
http://www.mendeley.com

<1% match (Internet from 23-Aug-2019)
http://gbata.org

<1% match (Internet from 09-Feb-2018)
http://faculty.cbu.ca

<1% match (Internet from 10-Jan-2018)
http://www.theijbm.com

<1% match (Internet from 28-Dec-2017)
http://isms-guide.blogspot.hk

Appendix B: Language Editor's Letter

EDITING LETTER

696 Clare Road
Clare Estate
Durban
4091
10 November 2020

To: Whom it may concern

Editing of PhD: Williams Adedayo Solomon (216069213)

INFORMATION SECURITY STANDARDS AND POLICIES COMPLIANCE BY NIGERIAN BANKS

This letter serves as confirmation that the aforementioned thesis has been language edited.

Any queries may be directed to the author of this letter.

Regards

[redacted]

MP MATHEWS
Lecturer and Language Editor
mercillenem@dut.ac.za
[redacted]

Appendix C: Ethical Clearance

UNIVERSITY OF KWAZULU-NATAL
INYUVESI YAKWAZULU-NATALI

18 March 2019

Mr Adedayo Williams (216069213)
School of Management, IT & Governance
Westville Campus

Dear Mr Wi liams,

Protocol reference number: HSS/0691/017D
New project title: Information security standards and policies compliance by Nigerian banks

Approval Notification – Amendment Application

This letter serves to notify you that your application and request for an amendment received on 15 March 2019 has now been approved as follows:

- Change In Title

Any alterations to the approved research protocol i.e. Questionnaire/Interview Schedule, Informed Consent Form; Title of the Project, Location of the Study must be reviewed and approved through an amendment /modification prior to its implementation. In case you have further queries, please quote the above reference number.

PLEASE NOTE: Research data should be securely stored in the discipline/department for a period of 5 years.

The ethical clearance certificate is only valid for period of 3 years from the date of original issue. Thereafter Recertification must be applied for on an annual basis.

Best wishes for the successful comp let on of your research protocol.

Yours [redacted]

Dr Rosemary Sibanda (Chair)

/ms

Cc Supervisor: Professor Manoj Maharaj
Cc Academic Leader Research: Professor Isabel Martins
Cc School Administrator: Ms Angela Pearce

Humanities & Social Sciences Research Ethics Committee
Dr Rosemary Sibanda (Chair)
Westville Campus, Govan Mbeki Building
Postal Address: Private Bag X54001, Durban 4000
Telephone: +27 (0) 31 260 3587/8350/4557 **Facsimile:** +27 (0) 31 260 4609 **Email:** [redacted]
Website: www.ukzn.ac.za

Appendix D: Questionnaire

COLLEGE OF LAW AND MANAGEMENT

SCHOOL OF MANAGEMENT, IT AND GOVERNANCE

UNIVERSITY OF KWAZULU-NATAL

PhD Research Project
SURVEY QUESTIONNAIRE

ISS COMPLIANCE BY NIGERIAN BANKS

Researcher: Williams Adedayo Solomon (+2778457527)
Supervisor: Prof. Manoj Marahaj (+27312608003)
Research office: Ms Ximba (+27312603587)

Introduction

Dear Sir/Madam,

You are humbly requested to complete the attached survey and return to me. This study investigates ISS Policy (ISSP) compliance among Nigerian banks. In addition, the compliance rates of Nigerian banks to FISMA, HIPAA, SOX, ISO/IEC 17799, and GLBA, are also examined. Where applicable, responses to the items in this survey are graded by a seven-point *Likert* scale. Please provide sincere and objective responses. There are no wrong answers, and your responses will be treated with utmost confidentiality and used for the purposes of this research only.

Consent

I hereby confirm that I understand the content of this document and the nature of the research project. I consent to participate in the research project. I also understand that I am at liberty to withdraw from the project anytime, should I so desire.

---------- ----------

Signature Date

Section I: Demographic Details

A. Your Job Description

_____

B. Years of Experience:	
Below 3 years	
From 3 to <6 years	
From 6 to <10 years	
10+ years	
C. Educational Level	
Diploma	
Bachelor's Degree	
Master's Degree	
Doctoral Degree	
Any other qualification	

Section II: ISSs Policies Compliance Rate

ISR01 How often does your organisation review its ISS Policy (ISSP) compliance?

Less often than once a year	At least once a year	At least once every 6 months	At least once every a quarter	At least once a month

ISR02 Which of the following international ISSPs does your organisation subscribe to? (Tick **ALL** that apply)

2.1 FISMA	
2.2 HIPAA	
2.3 SOX	
2.4 ISO/IEC 17799	
2.5 GLBA	
2.6 Other Specify _____	

ISR03 When last did your organisation adopt a new ISSs Policies (ISSsPs)?

More than a year ago	Between 6 months and a year ago	Between 3 and 6 months ago	In the last 3 months

Section III: Information Security Breach Experience

ISB01 How often does your organisation experience information security breach?

Less often than once a year	At least once a year	At least once every 6 months	At least once every a quarter	At least once a month

ISB02 Which of the following international ISSP, in your experience, successfully prevents an information security breach? (Tick **ALL** that apply)

2.1 FISMA	2.2 HIPAA	2.3 SOX	2.4ISO/IEC 17799	2.5 GLBA	2.6 Other: Specify

ISB03 When last did your organisation successfully avert a pending information security breach?

Never	More than a year ago	Between 6 months and a year ago	Between 3 and 6 months ago	In the last 3 months

Section IV: Perceived ISSsPs Compliance

Indicate your agreement with the following statements:		**Strongly Disagree**	**Disagree**	**Slightly Disagree**	**Neutral**	**Slightly Agree**	**Agree**	**Strongly Agree**
ISS 01	My organisation's Information security policy is consistently							
ISS 02	My organisation's information security policy evolves as							
ISS 03	There is a review system for our information security policy							
ISS 04	My organisation complies with major ISS policies							
ISS 05	ISS policy compliance is part of the organisation's core values.							

Section V: Normative Belief

Indicate your agreement with the following statements:		Strongly Disagree	Disagree	Slightly Disagree	Neutral	Slightly Agree	Agree	Strongly Agree
NOB 01	It is important to me for my co-workers to see me as an ethical							
NOB 02	My co-workers believe I should comply with information security							
NOB 03	I comply with inform security standard because my superior							
NOB 04	My co-workers believe it is important to comply with							
NOB 05	To my knowledge, the majority of employees comply with the							

Section VI: Information Security Threat Awareness

Indicate your agreement with the following statements:		Strongly Disagree	Disagree	Slightly Disagree	Neutral	Slightly Agree	Agree	Strongly Agree
STA 01	I clearly understand the implications of violating security policies.							
STA 02	I have received education about information security threats.							
STA 03	Information regarding security threats has been communicated to me							
STA 04	I know about a continuous awareness programme on general information security threat							
STA 05	Information security training was included as part of my orientation							

STA 06	Information security policies are discussed during my annual evaluation.							
STA 07	My supervisor updates me on changes to information security procedures.							

Section VII: Perceived Effectiveness of Information Security Policy Compliance

Indicate your agreement with the following statements:		**Strongly Disagree**	**Disagree**	**Slightly Disagree**	**Neutral**	**Slightly Agree**	**Agree**	**Strongly Agree**
PEF 01	Our information security policy is effective in achieving our organisational goals for information security.							
PEF 02	Our information security policy helps to accomplish the information security objectives.							
PEF 03	Our information security policy keeps the risk at a minimum.							
PEF 04	Compliance with the requirements of the information security, reduces security risks							
PEF 05	Compliance with the requirements of the information security policy (ISP) secures our infrastructure.							
PEF 06	Overall, the information security policy is effective in securing information at this organisation.							

Section VIII: Perception Biases

Indicate your agreement with the following statements:		Strongly Disagree	Disagree	Slightly Disagree	Neutral	Slightly Agree	Agree	Strongly Agree
PCB 01	In case of an information security threat, I always act swiftly no matter the severity of the threat.							
PCB 02	The measures in place to counteract information security threats are suitable and work successfully.							
PCB 03	The measures we use to counteract information security threats can successfully deal with the most complex of threats.							
PCB 04	The security-resisting mechanisms in place are successful in counteracting most threats that we experience.							
PCB 05	If I am unsure about a possible security threat, I prefer to take swift preventative measures rather than ignore it and have to fix it after it has happened							
PCB 06	The organisation sets high standards for the protection of its information assets							
PCB 07	Overall, compliance of the Information Security Policy at this organisation is good							
PCB 08	The policies in place regarding Information security are adequate to address security threats							

Section IX: Certainty of Detection

Indicate your agreement with the following statements:		Strongly Disagree	Disagree	Slightly Disagree	Neutral	Slightly Agree	Agree	Strongly Agree
COD 01	My computer practices are properly monitored for policy violations							
COD 02	If I violate the organisation's security policies, I will most likely be caught.							
COD 03	My computer is monitored for security threat exposure at random times of which I am unaware							
COD 04	I am assessed for information security compliance							
COD 05	My computer is routinely checked for security threat at regular intervals in time							

Section X: Severity of Penalty

Indicate your agreement with the following statements:		Strongly Disagree	Disagree	Slightly Disagree	Neutral	Slightly Agree	Agree	Strongly Agree
SOP 01	Employees caught violating security policies are appropriately corrected.							
SOP 02	Information security policies are enforced by punishing employees that break them.							
SOP 03	Serial information security offenders among the employees are appropriately disciplined.							
SOP 04	Employees who repeatedly break security rules can lose their jobs.							

SOP 05	If I were caught violating organisational information security policies, I would be severely punished.							
SOP 06	My employer takes strict action against violation of information security policy.							

Section XI: Employees' behavioural intention to comply

Indicate your agreement with the following statements:		**Strongly Disagree**	**Disagree**	**Slightly Disagree**	**Neutral**	**Slightly Agree**	**Agree**	**Strongly Agree**
EBI 01	In my daily work, I try to protect information and technology resources according to the requirements of the ISP of my organisation							
EBI 02	When I use information technology I try to carry out my responsibilities as prescribed in the ISP in order to ensure the security of the information I am working with							
EBI 03	When performing my daily work I try to comply with information security procedures.							
EBI 04	I tend to ignore information security procedures that I think are not necessary.							
EBI 05	My intention is to follow my organisational security policies wherever possible							

EBI 06	I intend to comply with information security policies.							

COLLEGE OF LAW AND MANAGEMENT

SCHOOL OF MANAGEMENT, IT AND GOVERNANCE

UNIVERSITY OF KWAZULU-NATAL, DURBAN, SOUTH AFRICA

Researcher: Williams Adedayo Solomon (+2778457527)
Supervisor: Prof. Manoj Marahaj (+27312608003)
Research Office: Ms Ximba (+27312603587)

RESEARCH FRAMEWORK VALIDATION QUESTIONNAIRE

Dear Sir/Madam,

I am a Ph.D. student of the above mentioned school, conducting a research on ISS Policy (ISSP) compliance in Nigerian banks.

This instrument is intended to be used for the verification and validation of the proposed model on information security standards and policies compliance in Nigerian banks.

Based on your experience in the banking sector, you have been selected to participate in the validation of the developed model (shown in Appendix A). You are implored to play an objective role in answering the questionnaire, with the belief that your tremendous contribution as a stakeholder will be invaluable to the banking sector.
.
However, voluntary response from your side will be given an utmost confidentiality, as the research is basically an academic-inclined one, without the attachment of any foreseeable risk.

Consent

I hereby confirm that I understand the content of this document and the nature of the research project. I consent to participate in the research project. I also understand that I am at liberty to withdraw from the project anytime, should I so desire.

---------- ----------

Signature Date

Section I: Demographic Details

Kindly tick the appropriate indicators in the shaded boxes.

A. Area of specialization: a. Head of operations ( ); b. ICT Personnel ( ); c. System maintenance officer ( ); d. Human resource manager ( ); f. Internal control officer ( ); g. Quality controller ( ); h. Executive manager ( ); i. Others ( ).
B. Years of experience: a. 10-15 years ( ); b. 16-20 years ( ); c. 21-25 years ( ); d. 26-30 years ( ); f. Above 30 years ( ).
C. Are you familiar with information security standards and policies in the bank?
a. Somehow familiar ( ); b. Familiar ( ); c. Very familiar ( ).
D. What is your level of involvement in information security standards and policies: a. Less than 25% ( ); b. 25-50% ( ); c. 51-75% ( ); d. Above 75% ( ).

Section 2. Validation of Research Model

The information security compliance model was developed after the analysis of the data collected during the research survey. The model was produced via factor analysis and regression analysis, while the significant items are as contained in the boxes in the attached model (Appendix A).

Based on your experience, kindly comment on the validity of the developed model in enhancing the compliance of employees to ISSsPs in Nigerian banks.

These questions require of you to mark the option that best suits your opinion with an 'X', in accordance to the scale provided, using the following rating scale as applied to questions 1 to 4 only: Strongly Disagree (1); Disagree (2); Slightly disagree (3); Slightly Agree (4); Agree (5); Strongly Agree (6).

Please indicate how you would rate the proposed model in relation to the following criteria.

1	**Appropriateness**	1	2	3	4	5	6
1.1	The model is in line with the policies and strategies of the bank.						
1.2	It enhances the effectiveness of the information security standards and policies of the bank.						
1.3	It can contribute to compliance of employees with information security standards.						
2	**Adequacy**						
2.1	Can address all the identified information security issues						
2.2	Can lead to the reduction of information security breaches.						
3	**Feasibility**						
3.1	Can be cost-effective						
3.2	Can be implemented within a short period of time						
3.3	Can be implemented with the available resources of the bank.						
4	**Flexibility**						
4.1	Can be easily adopted with changing policies.						
4.2	Can be adopted for mitigating information security threats within different branches of the bank.						

5.Intention to use

Please indicate the readiness of your bank to use the model.

No	**Description of Item**	**Yes**	**No**
5.1	Implementation of the model without changes.		
5.2	Readiness to adopt the model immediately.		

5.3	The usage of the model by the employees will be easy.		

NB: 'Easy' requires little or no training

6. Suggestions for improvement

6.1 If your response to 5.1 is '**No**', what changes will you suggest?.....
.....
.....

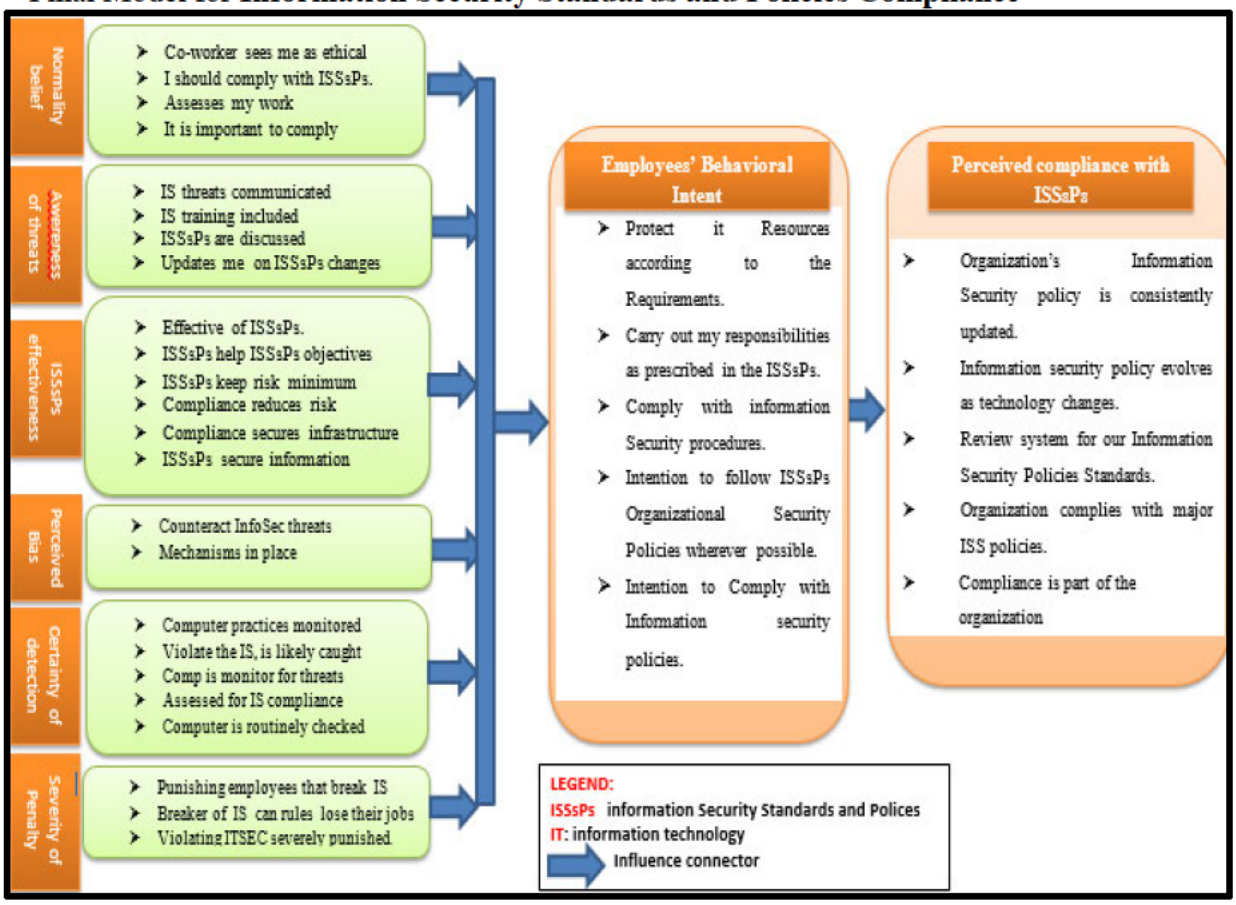
6.2 If your response to 5.2 is '**No**', provide reasons.....
.....

6.3 If your response to 5.3 is '**difficult**', provide suggestions for improvement.....
.....
.....

6.4 Recommend consideration of the information security policy issues that are not considered in the model.....

.....

Final Model for **Information Security Standards and Policies Compliance**



Thanks for your response.

Appendix E: Gate keepers' Letter

FirstBank
Since 1894

Centralised Processing Centre
Iganmu Complex, (5th Floor) 2 Abebe Village Road, Iganmu, Lagos, Nigeria
Telephone: Telephone: +234 1 8104723
Website: www.firstbanknigeria.com

22nd Feb, 2017
Mr. Williams Adedayo Solomon
School of Management, IT and Governance,
College of Law and Management,
University of KwaZulu-Natal,
Westville campus,
Durban,
South Africa.

Dear Sir,

RE: PERMISSION LETTER TO USE FIRST BANK AS A CASE STUDY

We reference to your letter Dated 19th Jan, 2017 on your request to use first bank as a research study. We understand that this is one of the requirements for the award of a Doctorate Degree programme. We are pleased to inform you that your request has been granted and we wish you success in your research work.

Thank you.
Yours faithfully
Aremu Julius
For: first Bank

[redacted]

VL/AIK/0414

FCT. Microfinance Bank Ltd.

...Promoting rural enterprise

10244

3rd , march 2017

Mr. Williams Adedayo Solomon

School of Management, IT and Governance,

College of Law and Management,

University of KwaZulu-Natal,

Durban,

South Africa.

Dear Adedayo,

RE: PERMISSION LETTER TO USE FCT BANK AS A CASE STUDY

We acknowledge the receipt of your letter Dated 26ST Jan, 2017 on your permission to conduct a research work on our organization. We understand that this is one of the requirements for the award of a Doctorate Degree programme.I amdirected to inform you that the management has approved your request. Also kindly notify the organization at least three week before the commencement of the research survey wishes you success in your research work.

Thank you.

Yours faithfully,

Aderibigbe Banji.

For: FCT Bank.

[redacted]

Head Office: Centre for Arts & Culture, Area 10, Garki - Abuja. Tel: 08034077484, +2348086157911, 08111811474

Guaranty Trust Bank plc
RC 152321
Plot 1400, Tiamiyu Savage Street,
Victoria Island,
Lagos State, Nigeria
Tel: 01 - 2627030-9, 2713192-6, 8986373
Tiamiyu Savage Branch FAX: 01-4480026
www.gtbank.com

15th march, 2017
Mr. Williams Adedayo Solomon
School of Management, IT and Governance,
College of Law and Management,
University of KwaZulu-Natal,
Durban,
South Africa.

Dear Adedayo,

RE: PERMISSION LETTER TO USE GTBANK AS ARESEARCH STUDY

In respect to your Letter Dated 23rd December, 2016 on permission to make use of our organization as a case study, we are aware that this is one of the prerequisite for award of doctorate degree. We therefore write to notify you that your request has been granted. We pray to give you support when the need arises. [redacted]

Best regards
Aremu Julius
For : GTBank [redacted]

Appendix F : Missing Data Table

Result Variables

	Result Variable	N of Replaced Missing Values	Case Number of Non-Missing Values		N of Valid Cases	Creating Function
			First	Last		
1	ISS01_1	2	1	355	355	SMEAN(ISS01)
2	ISS02_1	4	1	355	355	SMEAN(ISS02)
3	ISS03_1	2	1	355	355	SMEAN(ISS03)
4	ISS04_1	2	1	355	355	SMEAN(ISS04)
5	ISS05_1	2	1	355	355	SMEAN(ISS05)
6	NOB01_1	3	1	355	355	SMEAN(NOB01)
7	NOB02_1	2	1	355	355	SMEAN(NOB02)
8	NOB03_1	5	1	355	355	SMEAN(NOB03)
9	NOB04_1	3	1	355	355	SMEAN(NOB04)
10	NOB05_1	2	1	355	355	SMEAN(NOB05)
11	STA01_1	4	1	355	355	SMEAN(STA01)
12	STA02_1	4	1	355	355	SMEAN(STA02)
13	STA03_1	5	1	355	355	SMEAN(STA03)
14	STA04_1	11	1	355	355	SMEAN(STA04)
15	STA05_1	5	1	355	355	SMEAN(STA05)
16	STA06_1	5	1	355	355	SMEAN(STA06)
17	STA07_1	6	1	355	355	SMEAN(STA07)
18	PEF01_1	7	1	355	355	SMEAN(PEF01)
19	PEF02_1	5	1	355	355	SMEAN(PEF02)
20	PEF03_1	9	1	355	355	SMEAN(PEF03)
21	PEF04_1	9	1	355	355	SMEAN(PEF04)
22	PEF05_1	5	1	355	355	SMEAN(PEF05)
23	PEF06_1	5	1	355	355	SMEAN(PEF06)
24	PCB01_1	5	1	355	355	SMEAN(PCB01)
25	PCB02_1	5	1	355	355	SMEAN(PCB02)
26	PCB03_1	7	1	355	355	SMEAN(PCB03)
27	PCB04_1	6	1	355	355	SMEAN(PCB04)
28	PCB05_1	4	1	355	355	SMEAN(PCB05)
29	PCB06_1	6	1	355	355	SMEAN(PCB06)
30	PCB07_1	5	1	355	355	SMEAN(PCB07)
31	PCB08_1	6	1	355	355	SMEAN(PCB08)
32	COD01_1	5	1	355	355	SMEAN(COD01)
33	COD02_1	4	1	355	355	SMEAN(COD02)
34	COD03_1	4	1	355	355	SMEAN(COD03)
35	COD04_1	5	1	355	355	SMEAN(COD04)
36	COD05_1	4	1	355	355	SMEAN(COD05)

37	SOP01_1	4	1	355	355	SMEAN(SOP01)
38	SOP02_1	6	1	355	355	SMEAN(SOP02)
39	SOP03_1	4	1	355	355	SMEAN(SOP03)
40	SOP04_1	7	1	355	355	SMEAN(SOP04)
41	SOP05_1	4	1	355	355	SMEAN(SOP05)
42	SOP06_1	4	1	355	355	SMEAN(SOP06)
43	EBI01_1	5	1	355	355	SMEAN(EBI01)
44	EBI02_1	5	1	355	355	SMEAN(EBI02)
45	EBI03_1	5	1	355	355	SMEAN(EBI03)
46	EBI04_1	5	1	355	355	SMEAN(EBI04)
47	EBI05_1	5	1	355	355	SMEAN(EBI05)
48	EBI06_1	5	1	355	355	SMEAN(EBI06)

One sample test for the variable

One sample test for COD

	Test Value = 4					
					95% Confidence Interval of the Difference	
	t	df	Sig. (2-tailed)	Mean Difference	Lower	Upper
COD01 My computer practices are properly monitored for policy violations	12.927	349	.000	1.357	1.15	1.56
COD02 If I violate the organisation's security policies, I will most likely be caught.	16.462	350	.000	1.547	1.36	1.73
COD03 My computer is monitored for security threat exposure at random times of which I am unaware	16.043	350	.000	1.473	1.29	1.65
COD04 I am assessed for information security compliance	19.447	349	.000	1.649	1.48	1.82
COD05 My computer is routinely checked for security threat at regular intervals in time	18.263	350	.000	1.578	1.41	1.75