IMPLEMENTATION OF EFFECTIVE INFORMATION SECURITY MANAGEMENT STRATEGY TO PREVENT E-FRAUD

By

ZECHARIAH OLULEKE AKINPELU

A Dissertation submitted in partial fulfilment of the requirements for degree

MASTER OF BUSINESS ADMINISTRATION

At

Business School Netherlands

Internal Examiner: Dr Ayotunde Adebayo

Set: Ikeja 12

Set Advisor: Yinka Folami

Submission Date: 31st March, 2015

DECLARATION

I, **AKINPELU, ZECHARIAH OLULEKE**, hereby declare that this dissertation being submitted in partial fulfilment of the degree of Masters in Business Administration to Business School Netherlands is my own work. I have not submitted it for any degree or for any examination at any University or other institution.

ACKNOWLEDGEMENTS

I thank the Almighty God for the grace He gave me to run this programme successfully.

I acknowledge the following people:

Firstly, my loving wife, Stella Akinpelu for her immeasurable support, encouragement, assistance, and love that she gave me during the course of this programme.

My Dad, of blessed memory Pastor S.O Akinpelu who set the foundation for me, my mum, Deaconess E.A Akinpelu for her caring and understanding who supported throughout the research process.

I wish to thank the Business School Netherlands officials, the Managing Director, Prof. Pierre Strydom, Director of BSNN, Dr Lere Baale, my internal examiner, Dr Ayotunde Adebayo, Operations Manager, Mrs Morenike Adeyeye, Yvette Baker, and my set adviser, Yinka Folami.

My colleagues, Ikeja Set 12 for their support and direction. I love you all.

Finally, I thank my colleagues in Enterprise Bank Limited for their participation and timely feedback. God bless you all.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ACRONYMS

Acronym	Meaning	Abbreviation
ALMBA	Action Learning MBA	A unique MBA programme offered by the Business School Netherlands.
ALP	Action Learning Project	BSN approach of writing project that involves taking action and reflecting on the results
AMCON	Asset Management Company of Nigeria	A body established by Nigerian APEX bank to rescue distress bank
COBIT	Control Objective for Information and Related Technology	A set of objectives for Information Technology Governance
BSN	Business School Netherlands	An action learning MBA provider
CBN	Central Bank of Nigeria	An APEX bank that regulates other commercial bank activities in Nigeria
EBL	Enterprise Bank Limited	The researcher's organisation. One of the commercial bank in Nigeria
NEFF	Nigerian Electronic Fraud Forum	A forum found by CBN to discuss initiatives on how to combat e-fraud in Nigeria
NIST	National Institute of Standard and Technology	A federal institute that work with government to develop standard and apply standards
ISACA	Institute of Systems Audit and Control Association	A professional body that is involved in information security, IT audit, cybersecurity and IT Governance
IT	Information Technology	It is the application of computer to store, process and out data
PCI DSS	Payment Company Institution Data Security Standard	A set of standards for the protection of cardholder information

ABSTRACT

The purpose of this dissertation was to implement an effective information security strategy to prevent e-fraud in Enterprise Bank Limited, a commercial bank in Nigeria. The research applied three theoretical frameworks - the NIST Cybersecurity, COBIT 5 for Information Security and PCI DSS. Following literature reviews on the subject matter, the study used a survey design that involved qualitative techniques. The methods used were a group strategy discussion session involving some management staff of the bank, and, interviews team leads of staff whose jobs' functions are related to the management of information security in the bank. The discussions and the interviews were guided by scripts that the researcher developed. The scripts were based on the research questions and literature reviews. The information obtained from the surveys were analysed and used in answering the research questions. Twelve senior staff - team leads of units whose functions were related to management of information security were interviewed. Six management staff were also engaged in group discussion to examine the current information security management strategy in EBL with comparison to best practice and establish security gaps in the bank, establish the consequence of those gaps on the bank's information asset and provided solutions on how to prevent e-fraud. The result of the researched revealed that ineffective information security management strategy in the bank resulted in escalating e-fraud in the bank. The research also recommended the adoption of NIST Cybersecurity framework to make the bank's information security strategy effective and be able to combat e-fraud.

Keywords: *Cybersecurity*, *COBIT 5, Preventive Control,Corrective Control, Deterrent Control, Detective Control, Compensating Control, Confidentiality, Integrity, Availability, ISO 27001*

CHAPTER ONE

1.0 INTRODUCTION

1.1 BACKROUND OF STUDY

A financial organisation with effective information security strategy is less prone to data leakages and consequences of not implementing the strategy such as phishing attack, hacking, social engineering etc. Information Security management strategy is very crucial towards the protection of organisational and customers' data. COBIT 5 frameworks for information security is one the model used to establish the effectiveness of information security strategy in an organisation. COBIT 5 provides a comprehensive ways of ensuring reasonable and appropriate security control for information resources (ISACA, 2012). National Institute of Standard and Technology (NIST) (2014) established cybersecurity framework. The framework helps organisations to apply principles and best practices of risk management to improving the security and resilience of critical infrastructure which include organisational and customer data and preventing electronics fraud.

The Central Bank of Nigeria (CBN) established Nigerian Financial Services IT Standards Blueprint. The standards contain different IT/Information Security framework to be adopted by Nigerian financial institution which include the objectives and intention, description, minimum acceptable maturity level, derivable benefits, requirements for compliance, consequences for deviation and timelines for compliance. The figure below shows the CBN IT roadmap for all banks and timelines. It is expected for all banks to achieve a minimum maturity of 3 out of 5 on or before deadlines as show in the figure below.

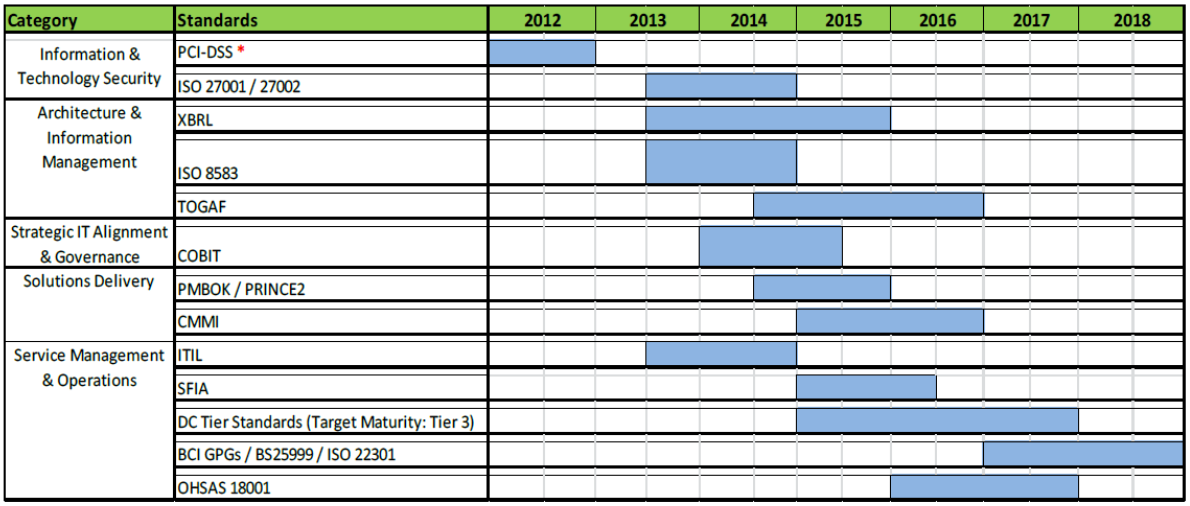

Figure 1.1: CBN IT Roadmap and Timelines

Source: CBN IT Standards and Blueprints, 2013

Retrieved February 1, 2016 from http://www.cenbank.org/ITStandards/IT_Standards_Blueprint_Final_revised%204%20website.pdf . The following are the maturity level of the CBN information security standards of three financial institutions based on the audit conducted by the apex banks examiners.

S/N	Banks	PCI DSS Maturity	ISO 27001 Maturity	COBIT 5 Maturity
1	Wema Bank	4	3	4
2	Sterling Bank	3	4	4
3	Enterprise Bank	2	2	1

TABLE 1.1: CBN Assessment of Bank's Information Security Standards

Enterprise Bank Limited (EBL) was incorporated in August 2011. The asset and liabilities of the formal Spring Bank Plc. was taken over by the bank as a result of Central Bank of Nigeria intervention to rescue the defunct Spring Bank. CBN revoked Spring Bank's license as result of an industry-wide audit, the bank was one of the banks that were under-capitalized and badly managed. The new bank was licensed as a commercial bank by the Central Bank of Nigeria, the country's banking regulator. The bank is owned by Asset Management Company of Nigeria (AMCON), an arm of the Federal Government of Nigeria. The bank was fully recapitalised by Asset Management Company of Nigeria (AMCON) with an injection of N12 billion. It has an additional asset base of N280 billion which gives the new bank a strong competitive edge among other commercial banks in the country. The vision of the bank is to "To be the preferred bank for value creation" and mission is "To delight our stakeholders through a highly motivated workforce using innovative solutions". EBL core value is coined from "A new SPIRIT" which is stated: S – Service Excellence, P – Professionalism, I – Innovation, R – Respect for Individual, I – Integrity, T – Teamwork. Retrieved July 11, 2014 from http://www.entbankng.com.

The researcher is the Head, IT Security & Compliance. He is responsible for coordinating the governance, risk, control and compliance in the IT department.

In Enterprise bank, strategy towards information security to safeguard the organisation and customer data is not effective which poses serious financial and reputational threat to the bank.

This was revealed by the data captured by the bank's customer management unit. The customer service management recorded about 67 reported customers' data that were compromised via the bank's electronic channels in 2014. In April, 2013 the bank's electronic platform was defrauded of N21, 000,000.00 as a result of lack of measure to safeguard the bank's data. Between May, 2013 and October, 2014 the bank furthermore recorded another two – similar electronic fraud (e-fraud) occurrences which exposed the bank to the loss of about N672,000,000.00 because no effective measure were taken to mitigate the existing risk source. The CBN capability maturity level examination among peers financial institution as shown in the table 1.1 above also revealed that the EBL information security strategy is not yet mature.

1.2 STATEMENT OF PROBLEM

Information security strategy towards prevention of e-fraud in EBL are of great concerns due to the escalating fraud that occurs on the bank's e-platform.

1.3 PURPOSE OF STUDY

The purpose of this study was to develop an effective information security strategy to prevent e-fraud in Enterprise Bank Limited.

1.4 RESEARCH OBJECTIVES

Arising from the purpose of study, the following research objectives was determined:

1. To understand and examine the current information security management strategy in EBL with comparison to best practice
2. To establish information security gaps in EBL
3. To establish the consequence of those gaps on the bank and its information asset
4. To recommend effective ways by which bank's e-fraud can be prevented as informed by best practice.

1.5 RESEARCH QUESTIONS

1. How information security management is practiced in EBL?
2. What are the gaps of information security management strategy in EBL?
3. What are the consequence of these gaps on the bank and its information asset?

4. How can the bank prevent e-fraud?

1.6 THEORETICAL FRAMEWORK

This study was inspired by three framework which are Cybersecurity framework, COBIT 5 framework for information security and PCI DSS Framework

1.6.1 CYBERSECURITY FRAMEWORK

This study was inspired by framework for improving critical infrastructure (National Institute of Standards and Technology, 2014). The framework focused on how to use business drivers to guide security activities considering risk as part of the organisation's risk management process. The framework helped organisations to apply principles and best practices of risk management to improving the security and resilience of critical infrastructure/data which include organisational and customer data. The Framework Core four elements which were functions, categories, subcategories and informative references. The five concurrent and continuous functions are Identify, Protect, and Detect, Respond, and Recover which together provided a high-level, strategic view of the lifecycle of an organisation's management of cybersecurity risk as shown in figure 2 below.

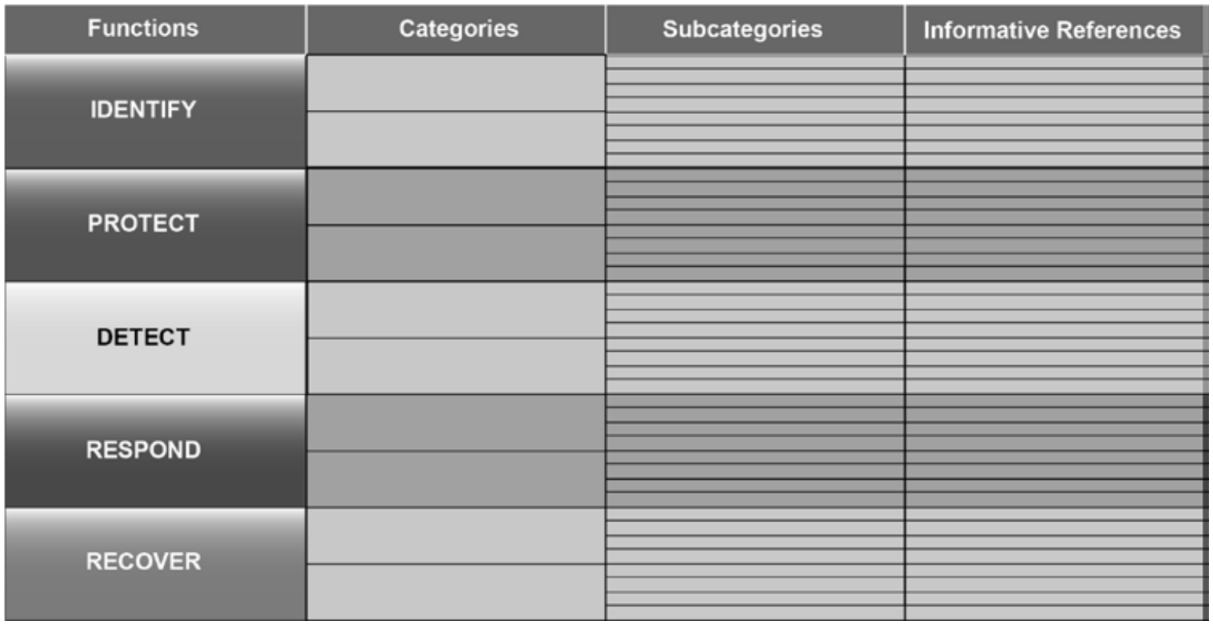

Figure 1.2: Cybersecurity Core Framework

Source: Framework for Improving Critical Infrastructure Cybersecurity, NIST, USA, 2014

1.6.2 COBIT 5 for Information Security Framework

COBIT 5 for Information Security an ISACA publication (2012) highlighted the major drivers for the development of Information Security and benefit of COBIT 5. The framework provided a comprehensive ways of ensuring reasonable and appropriate control for information resources. It was based on five guiding principle as illustrated in the figure below:

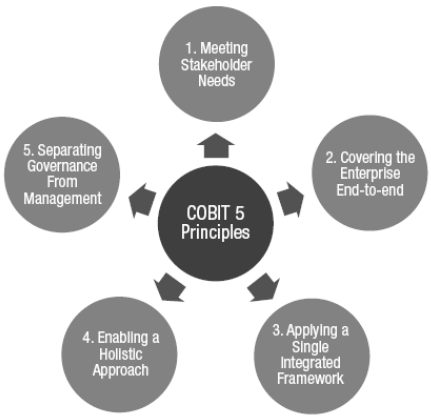

Figure 1.3: COBIT 5 Framework for Information Security Principle (ISACA, 2012)

1.6.3 PCI DSS Framework

PCI DSS provided a baseline of technical and operational requirements to protect cardholder data information data. The standard specified twelve requirements for compliance. This compliance was organised into six control objectives as shown in table 2 below. Retrieved December 17, 2015 from https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-1.pdf

1.7 LIMITATION OF STUDY

The bias in this study shall be as a result of the researcher's involvement. Since the researcher is the head, IT security of the company, there is the likelihood that the researcher's own assumptions and opinions, may be the source of some bias to the research carried out.

1.8 SIGNIFICANCE OF STUDY

This study would be useful to the Board and Management of Enterprise Bank Limited, as it would provide the company with essential information to aid its success. It would also be useful to the management of other commercial banks in Nigeria that are considering information security strategies for preventing e-fraud.

1.9 SCOPE AND DELIMITATION

The study focused on four departments that are saddled with the management of information security in the bank. The delimitation of the study was that it did not cover all the branches/units of the bank.

1.10 RESEARCH PROCESS

This research used qualitative methods. It entailed a survey design comprising of two parts: A group discussion strategy session with the senior management of the bank whose oversight are related to management of information security or information systems and e-business and

Interview sessions with the team lead leads (senior officers) whose jobs' functions are related to the management of information security.

During the group discussion session, the management staff reviewed the current information security management strategy in the bank, identified the gaps in the current practice and consequences of those gaps. Thereafter, they concluded on how to prevent the e-fraud in the bank based on the outcome of the discussion.

In conducting the in-depth interviews with the team leads of the staff responsible for the management of information security in the bank, the researcher had a one on one discussion with each person (this will be later attached in this research). The objective of the meeting was to get more insight in choosing a viable option to ensure that e-fraud were prevented in the bank.

The information obtained from the group discussion session and in-depth interviews was analysed and used in answering the research questions. It also helped to understand the urgency in implementing effective information security strategy

1.11 DEFINITION OF TERMS

Availability: It is a term in information security that ensures reliability and timely access to data and resources to authorised users

Confidentiality: It is term term in information security to ensure that information is not disclosed to unauthorised individuals, processes or systems

Control Objective for Information and Related Technology (COBIT): A set of objectives for Information Technology Governance

Cybersecurity: Is the process of protecting information/data by preventing, detecting, and responding to attacks

E-Fraud: Fraud related to the use of technology

Enterprise Bank Limited: The researcher's organisation

Integrity: It is term term in information security that ensures the accuracy and reliability of information and systems.

PCI DSS: A set of standards for the protection of cardholder information

1.12 CHAPTER LAYOUT

The layout of the dissertation comprises of seven chapters. Chapter one covers the Introduction and Problem Statement of the dissertation. Chapter two contains the Literature Review. Chapter three provides information about the Research Methodology while chapter four shows the Results and Findings. The fifth chapter looks at the Evaluation of Options and Recommendations, while chapters six and seven cover the Implementation Plan and the Researcher's Reflection, respectively.

1.13 CONCLUSION

This chapter provided a background to this study. It highlighted the objectives and significance of the study. It also provided a summary of the research plan.

The next chapter would review relevant literature written on the various elements of the research variables of this study. The following chapter considers the methodology and the process that was used in the research.

CHAPTER TWO

2.0 LITERATURE REVIEW

2.1 INTRODUCTION

This chapter focused on the intensive review of literature conducted on the research topic. For a better understanding of the research topic, extensive work was done on the findings. Theories and write-ups from several articles and journals which were from the EBSCO library, information security source materials, textbooks, search engines and other relevant sources, which helped form an extensive understanding of information security management strategy to prevent e-fraud in EBL.

2.2 INFORMATION TECHNOLOGY AND INFORMATION SECURITY

According to Haag and Cummings (2013), the manner at which people utilize technology can and, in fact, does change the competitive landscape of business in a significantly. Technology affects our style of doing things and the way of life as we rely on it for our daily routines. Every part of our lives and what we do depend on technology. Technology drives most of our electronics devices such as smart TV, mobile phones, tablets, music players and cannot be fully utilised without the use of technology. The impact of technology is significant, and it is changing the entire industry.

Technology has been so much part of our lives that we may consider it more of a necessity than a convenience. We cannot imagine life without a cell phone, having to do without text messaging for a week or having the Facebook's website shutdown. The pace of development and transformation in IT is fast and not comparable to how it uses to be. (Haag and Cummings: 2013).

Information technology (IT), according to Haag and Cummings (2013), is any computer-based tool that people use to work with information and support information and information-processing needs of an organisation. IT is simply a set of tools that helps you work with and process information.

Fabian (2003) stated that IT is giving required competitive advantage. In recent years, banks have been investing more in IT, not only as a means to reduce costs and improve operations but as a key to profitability. With IT, banks can improve their management of customer relationships, streamline operations, expand their activities, minimise risk exposures in a

turbulent market and improve services. The software solution is helping to optimise branch delivery through facilitating the planning of new sites, relocations and closures based on a host of detailed data, such as population demographics and density.

There has been a transformation in the delivery of services as a result of reliance on IT as this has improved the quality of service offerings. The role of technology in service organisations has been primarily employed to cut down costs and remove doubts. Technology has been used in the service sector to bring about standardization by reducing human interfaces which are prone to error. Most consumers now prefer to embrace the use of technology-based service delivery over that of the employee. This new development and issues arising from it as it affects service quality and customer satisfaction (Mathew, Cindy, and Beatriz: 1999).

Due to the expansion of the scope of IT beyond the traditional boundaries, information security management has become intricately integral part of the organisation. For example, inter-organisational information systems primarily physically connect firms' IT infrastructure via the web and expose the participating firms to network-wide security risks. An organisation's network is at risk if a malicious person gains access to its partner's network. Even firms without close business relationships may be logically interdependent: Strategic hackers often evaluate the security level of enterprises and select their targets by whose systems they can break into quickly without notice. A company's security risks depend not only on its security practices but also on the protections of others (Zhao, Ling and Whinston, 2013).

2.2.1 ELECTRONIC BANKING IN NIGERIAN FINANCIAL INSTITUTIONS

According to Fabian (2003), globalisation has brought intense competition in the financial services industry. This contest has the tendency to bring out the best in the financial institutions. To remain competitive, they need the flexibility to be able to respond rapidly with new products to fast-changing market needs. One major challenge is how to meet the increasing expectations of customers. The retail banking industry, in particular, has become completely transformed. All banks' activities used to occur in the branches, and customers' access to financial services were limited to hours of operations. Each branch represents the bank. The Nigerian banks are under pressure from the forces of globalisation to adopt Information technology to fit into the evolving global banking system. So the motivation is principally that of survival. In the absence of an indigenous IT culture and a significant user-producer relation, the banks could not rely on internally developed products nor could they maintain a balanced interaction between business objectives and IT innovations. We have seen the effects of a panic and ad

hoc implementation of information systems. They include under-utilisation or non-utilisation, inappropriate "solutions", frequent downtime, complete failure, and frustration. The current level of investment in and implementation of IT is not impressive, and very few banks can claim to have realised some of their expectations in investing in IT (Fabian: 2003). The adoption of electronic payment system is on the increase as a result of CBN policy for cashless Nigeria as revealed in the volume of transactions processed in the country using payment cards and other e-banking platforms over the years; even though the dependency on cash is still relatively high. Retrieved February 4, 2016, http://cbn.gov.ng/Out/2016/CCD/NEFF%202014%20Annual%20Report%20.pdf .

According to Usman and Shah (2013), electronic banking has to do with rendering banking services through electronics means such as online banking, automated teller machine (ATM), Electronic Funds Transfer, Electronic Cheque Conversion and Web ATM services. With the increase in the use of e-banking services and its technological risk, is important to look at how to mitigate this risk. The critical success factor for e-banking is information security. The inadequate of information security strategy leads to a financial loss in e-banking.

2.2.2 CONCEPT OF INFORMATION SECURITY MANAGEMENT

Information security management is the administrative and procedural activities necessary to support and protect information and organisation assets throughout the enterprise. It involves development and enforcement of security policies and their supporting mechanisms: procedures, standards, baselines, and guidelines which encompass enterprise security development, risk management, proper control selection and implementation, governance, and performance measurement. Effective information security management guaranteed the confidentiality, integrity and availability of information asset (Harris, 2013).

According to the Committee on National Security Systems (CNSS), as sighted in Whitman and Mattord (2012), information security is defined as the protection of information and all its elements. These elements are systems and hardware that are used to store or transmit the information. The CNSS model evolved from the basic concept of information security which is the confidentiality, integrity and availability (CIA) of information assets. Information security involves different components which can be network security, data security, application security, policy, etc. as illustrated in figure 2.1 below.

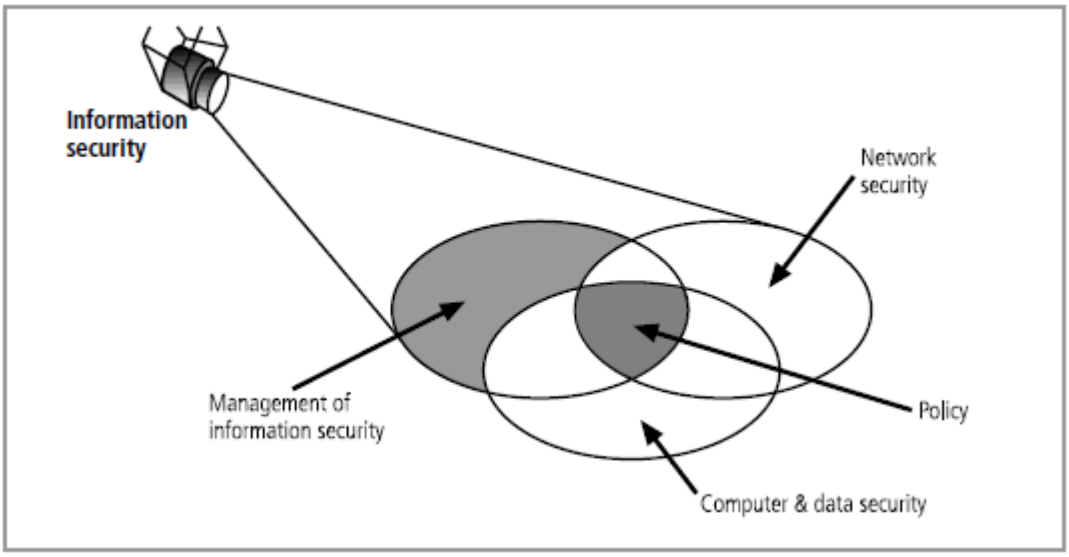

Figure 2.1: Component of Information Security

Source: Course Technology/Cengage Learning (2011)

Information security is a safeguard that can be applied to manage IT risk in an organisation. The objectives of information security are to ensure the availability, integrity, confidentiality and protection of critical assets as illustrated in figure 2.2 below. Availability ensures reliability and timely access to data and resources to authorised users. Integrity ensures the accuracy and reliability of information and systems. It gives assurance of unauthorised modification to information systems or data. Confidentiality is to ensure non-disclosure of information from unauthorised individuals, processes or systems (Harris, 2013). Information security gives the enterprise assurance that information is protected against disclosure by malicious users (confidentiality), improper modification and non-access when required (availability) (COBIT, 2012).

Mishra and Robert (2011), described how three constructs: security policies, deterrence practices and systems auditing can impact information security effectiveness as illustrated in figure 2.2 below

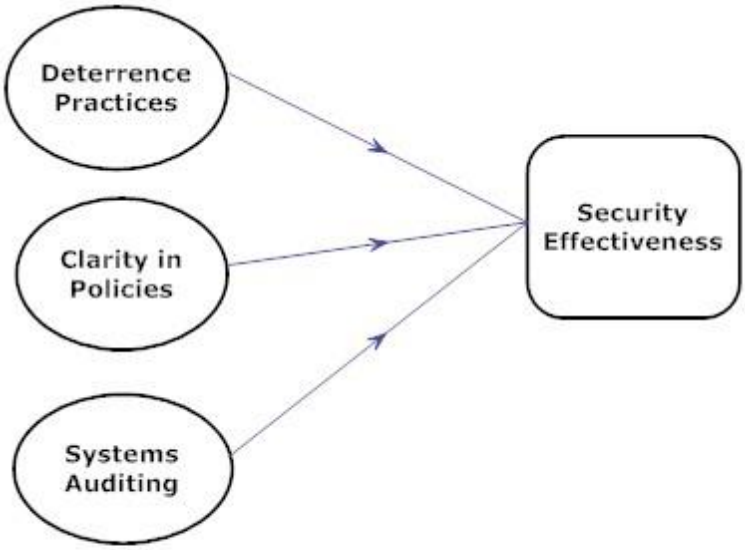

Figure 2.2: Security Effectiveness in Organisation (Mishra and Robert, 2011)

According to the model, deterrence activities establish strict criteria to enable employees to understand acceptable security actions and behaviour in the organisation. It enables the employees to understand the consequence of their actions and results of non-compliance to IT security standards. Management should ensure the clarity of various IT security policies and procedures to ensure the effectiveness of the implementation of IT controls. Systems auditing provides independent assurance of the governance, risk and control of an organisation to determine the maturity of the efficacy of the various IT security control (Mishra and Robert, 2011).

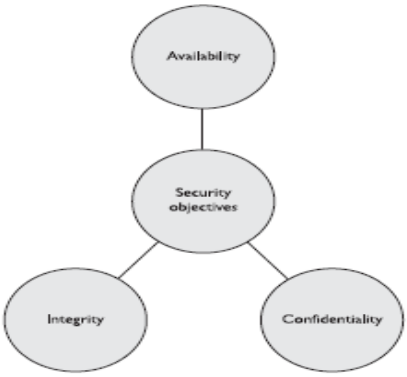

Figure 2.3: Fundamental Principle of Information Security (Harris, 2013, 22)

2.2.3 PROTECTION OF INFORMATION ASSET

According to Zhao and Johnson (2010), managing of information in highly dynamic e-business environments is increasingly challenging. With increasing large organisation with staff accessing lots of applications and data sources, it is imperative for the management to protect information against misuse but ensure that staff can access the information needed to create

value. Cybersecurity is the process of protecting information/data by preventing, detecting, and responding to attacks (NIST, 2014).

The interdependency of information security makes the most organisation to invest inefficiently in information security management. Cyber insurance seems to be a promising solution to help organisation optimise spending. However, this is ineffective in addressing investment inefficiency caused by risk interdependency. Two alternative risk management approaches are preferred which are risk pooling arrangements (RPAs) and managed security services (MSSs). Association can utilize a RPA as a supplement to digital protection to relieve the probability of overinvestment issue brought about by negative externalities of security ventures; be that as it may, the appropriation of an RPA is not motivating force perfect for firms when the security speculations create positive externalities. MSS supplier serving different companies can disguise the externalities of security speculations and moderate the information security venture wastefulness. As an aftereffect of danger interdependency, aggregate outsourcing emerges as a harmony just when the total number of firms is little (Zhao et al, 2013).

According to Harris (2013), information security control/protection is the safeguard that is put in place to mitigate a risk. These controls are in three categories which are administrative, technical and physical. Administrative controls are management oriented this can be security documentation, risk management, personnel security and training. Technical controls are also known as logical control; these are software and hardware components which can be antivirus, firewalls, biometrics, smart cards and encryption mechanism. Physical controls are things instituted to secure office, faculty, and assets. Samples of physical controls are security guides, locks, fencing, and lighting. All these three control put in place provide defence in depth- a coordinated use of multiple controls in a layered approach as shown in figure 2.3 below.

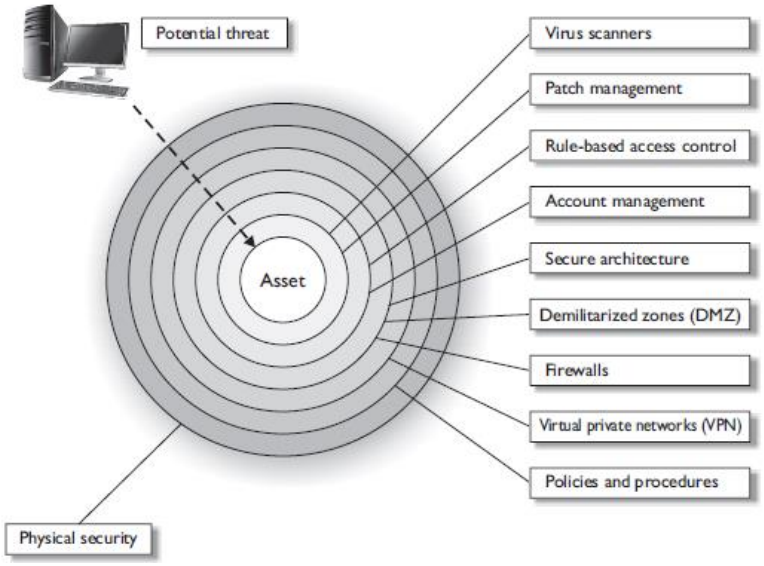

Figure 2.4: Defence in Depth (Harris, 2013, 29)

Different functionalities of controls are preventive, detective, corrective, recovery and compensating controls. She further explained that for one to make an informed decision on the right controls for a particular situation one has to understand the controls functionalities. The control functionalities are: Deterrent controls discourage a potential attacker; Preventive controls prevent events from occurring; Corrective controls fixes systems after an occurrence; Recovery controls bring the environment back to regular operations after incidence; Detective controls help identity malicious activities, and potentially an intruder and Compensating controls provide an alternative measure of control (Harris, 2013).

According to Klie (2015), protecting organisation's valuable data should begin from contact centre staff and end in the top management. The target of hackers is the large-scale data which comprises customers' data such as credit cards, social security numbers, names, addresses, employment records. These data are seen as gold mines which are traded to interested people. It is imperative for the organisations to ensure that countermeasures are built on their infrastructure. Despite the alarming growth of attacks on customers' personal and financial information, many companies are not putting a countermeasure for securing data in place. The following are suggested to safeguard organisation's data (i) creation of incident response and crisis management; (ii) this first point is achievable by having a high level executives that is responsible for data security (iii) data inventory to determine the sensitivity of the data (iv) systematic purge of the data that are no longer needed and a push for the Payment Card Industry Data Security Standards (PCI DSS).

PCI DSS are sets of information security conventions that incorporate rules for building and keeping up secure information systems, ensuring cardholder information, controlling access to the information, observing and testing systems to guarantee that data security arrangements are kept up and implemented (Klie, 2015).

2.2.4 INFORMATION SECURITY MANAGEMENT SYSTEMS (ISMS)

An ISMS is a way of managing an organisation' critical data with a set of policies and procedures to manage risk to an acceptable level and ensure business continuity Retrieved February 2, 2016 from http://searchsecurity.techtarget.in/definition/information-security-management-system-ISMS. International Organisation for Standardization published ISO 27001:2013 standard defines the requirements for setting up, actualizing, keeping up and ceaselessly enhancing information security administration framework (ISMS) inside of the connection of a foundation (ISO 27001:2013). The standard gives customers, staff and third parties or suppliers assurance that organisation maintains an effective security management which helps in a proactive measure to deal with security threats and issues (Freeman, 2007). According to ISO 27001 (2013), the requirements for the management of ISMS as explained in the table below

S/N	REQUIREMENT	EXPLANATION
1	Context of the Organisation	The context of an organisation is the environment where an enterprise can achieve its objectives which can be internal or external. Examples of internal context are organisation governance, policies, culture, standards, etc. The external context can be the cultural, social, political, etc. Retrieved March 1, 2016 from http://iso27001security.in/clause-4-1-understanding-the-organisation-and-its-context/
2	Leadership	Top management and business executives commitment are crucial to achieving effective ISMS as they will ensure strategic alignment of information security objectives with business objectives, ease integration of information security requirement into organisations processes, formulation and driving of information security policies

		and to ensure that roles, responsibilities and authorities are assigned and communicated
3	Planning	An organisation should ensure that there are actions to address risk and opportunities to ensure that ISMS achieves its objectives, reduce risk to an organisation acceptable level, ensure continual improvement of ISMS and risk is adequately treated and communicated to all stakeholders.
4	Support	The organisation is required to provide adequate resources for the establishment, implementation and continual improvement of ISMS. This is achieved by ensuring that staff who are responsible for the management of ISMS are adequately trained, or engaging competent personnel's, end users are aware of the information security policy and consequences of non-compliance. To ensure organisational support to ISMS, external and internal communication is crucial to all stakeholders.
5	Operation	It is very important for an organisation to ensure planning, implementing and controlling process required for effective management of information security. Risk assessment needs to be conducted periodically or whenever major changes occur, and the result should be well documented. Risk treatment plan needs to be put in place and well documented.
6	Performance Evaluation	To determine the performance and the effectiveness of ISMS, security processes and controls need to be monitored at the definite time by trained personnel and the results need to be evaluated and analysed as appropriate. The role of internal auditor is also critical to determine the effectiveness of ISMS. The audit needs to be conducted at plan intervals, scopes and criteria need to be clearly defined and results need to be communicated to appropriate management. Top management overview is one of the

		critical success factors for effective ISMS. Management review needs to be carried out at planned interval to determine the status of the action plans for previous reports, oversight of all changes relevant to information security, actions taken against non-conformity, feedbacks from audit, etc.
7	Improvement	To ensure continuous improvement of ISMS, there should be corrective action to react nonconformity, deal with the cause of non-conformity, review the effectiveness of any action taken and document all information as evidence of traction.

Table 2.1: ISO 27001:2013 Requirements

It also defines the requirements for defining IT security risks and how an organisation can respond to risk with a risk treatment plan by choosing appropriate controls (ISO 27001:2013). These controls are explained in the table below:

S/N	CONTROLS	EXPLANATION
1	Information security policies	Give administration heading and backing to information security in arrangement to business objectives
2	Organisation of information security	Manage information security within the organisation
3	Human resource security	These controls ensure that employees responsibilities in order to reduce risk of theft, fraud and misuse of facilities
4	Asset management	Control to achieve and maintain appropriate protection of organisation assets
5	Access control	To control access to information

6	Cryptography	To secure the privacy, uprightness or accessibility of data by cryptographic means
7	Physical and environmental security	To prevent unauthorised physical access to organisation's premises or information
8	Operations security	To ensure the correct and secure of information processing facilities
9	Communications security	To ensure information security when using communication device
10	System acquisition, development and maintenance	To ensure that security is an integral part of systems development life cycle
11	Supplier relationships	This controls ensure that contractors and suppliers understand their responsibilities in order to reduce risk of theft, fraud and misuse of facilities
12	Information security incident management	To ensure that security incidence is communicated timely to ensure that actions are taken
13	Information security aspects of business continuity management	To prevent loss of information asset in the event of disaster
14	Compliance; with internal requirements, such as policies, and with external requirements, such as laws	This is to avoid breaches in any law, statutory, regulatory or contractual obligations of any security requirement

Table 2.2: ISO 27001:2013 Controls

2.3 INFORMATION SECURITY MANAGEMENT STRATEGY

Ricky and Monique (2014) defined security strategy as a roadmap for establishing information security practices that can be used to meet future challenges as the attacks vectors such as hacking, electronic fraud (e-fraud), phishing are on the increase. It is very necessary for the organisation to determine current security status to set achievable goals based on the long-term strategic mapping. They identified six steps of developing security strategy which are: (i) Posture and Establishing Asset value – identifying the current and desired future security posture, determining the cost of asset and its importance to business (ii) Assessing the exposure – this entails assessment of people, process and technology in order to determine where changes need to be made to ensure a workable future security strategy (iii) Analyse the security information gathered – this helps in identifying missing safeguards (iv) Plan and Develop a Security Strategy – this has to do with the conversion of analysis into security strategy (v)Strategic Alignment – this helps in continuous evolution and improved processes and security posture (vi) Communicate the Security Strategy – this is very essential to ensure that everybody within the organisation is armed with the knowledge of information security. The awareness is aimed at management, staff and technical employees.

Information security is not only about firewalls, intrusion detections systems (IDS), security incidence and event monitoring (SIEM) antivirus software or passwords; it is a continuous process or journey which requires management persistence to ensure that things are working the way it supposed to be (Ricky and Monique, 2014). LeVque (2006) information security strategy is focused on building business trust relationship to ensure confidentiality, integrity and availability of business transaction and data. Planning and preparation are very important to develop an extremely effective information security strategy as illustrated in figure 2.4 below. According to Young and Windsor (2010), an organisation that has a mature information security strategy exhibits a robust planning process such as management and user involvement which leads to more efficient security implementations.

:

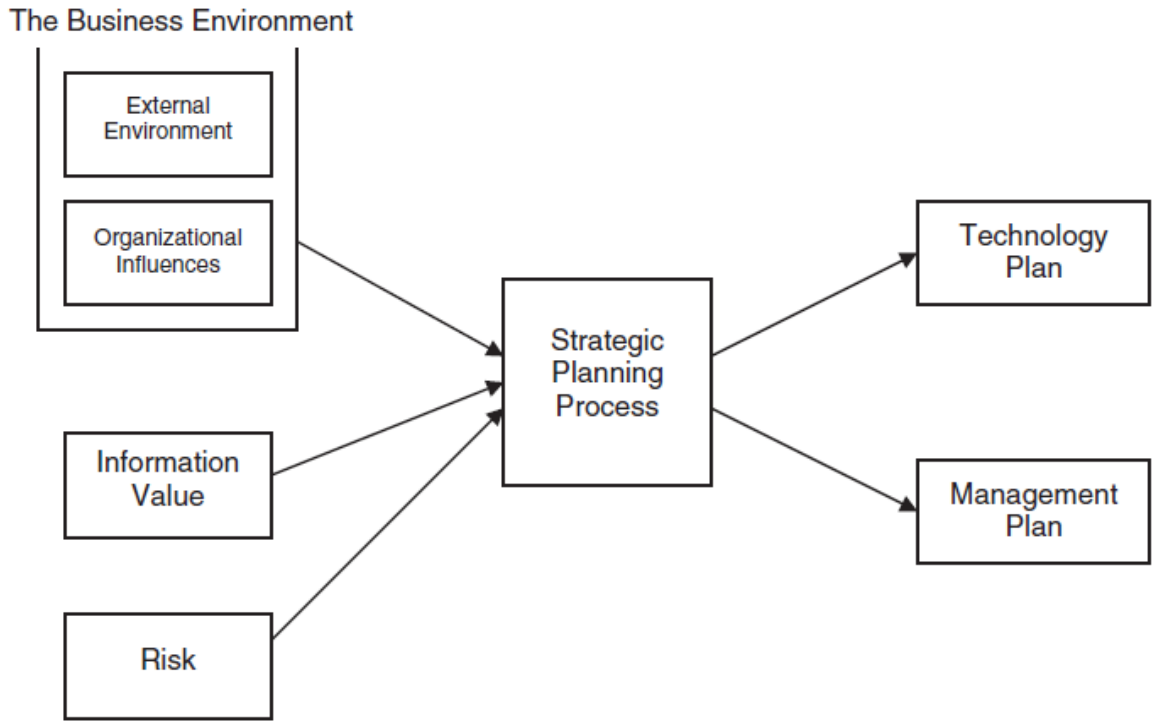

Figure 2.5: Information Security Strategic Planning Model (LeVque: 2006)

According to Pironti (2010), an information security strategy is a roadmap for the protection of the organisational information asset with the goals to ensure that capabilities provided are aligned with business goals and risk profile. He describes a multiphase approach to developing as information security management strategy which are: Phase I – Business Awareness; Phase II – Strategy definition; Phase III – Strategy Development; Phase IV – Metrics and Benchmarking; Phase V – Implementation and Operation (Pironti, 2010).

2.3.1 PHASE I - BUSINENESS AWARENESS

The first phase of information security management strategy includes an understanding of the organisation current business condition and risk profile and appetite. The current business conditions enable the organisation to be able that has been defined. As information security strategy is to complement the company goal, it is also crucial to maintain a responsible level of risk management the goal. Aligning with enterprise risk management (ERM) gives the business comfort that the strategy is business enabling (Pironti, 2010). The first thing to do in security strategy is the identification of the dominant threat and rank those threats in order prioritise as necessary (Whitman, 2003).

2.3.2 PHASE II – STRATEGY DEFINITION

The second phase of information security management strategy includes a tactical plan (annual) and strategy plan (30-36 months plan). It allows the organisation to understand the current state of capability as well as its projected needs and requirement for future. Different purposes of landing for survey and choice by the association's administration group and key execution markers (KPIs) given the chosen purpose of entry to screen worth and viability should be recognised which guarantees the accessibility and capacity of staff that will execute technique and addition a comprehension of the association's way of life to guarantee a proper arrangement for information security administration methodology reception (Pironti, 2010).

2.3.3 PHASE III – STRATEGY DEVELOPMENT

The third phase includes the definition of the governance model and functional capabilities and service that will be provided by the organisation. This phase defines consideration whether the information security strategy will include operational components or will act as a consultative element within the organisation. It defines determination of the reporting structure; it also defines the consideration of the staff and their competency to successfully implement the strategy and consideration of the risk of sourcing and ensure adequate oversight by internal staff (Pironti, 2010).

2.3.4 PHASE IV – METRICS AND BENCHMARKING

The fourth phase includes alignment with the industry standard such as COBIT, ISO 27000, NIST, etc.; using the capability maturity model (CMM) assessment methodology and use KPIs to measure the effectiveness of the implemented strategy. The CMM system (see figure 2.4) is a successful approach to comprehending which of its abilities are satisfactory and which require a territory of change so as to build effectiveness, diminish the expense of operation and expansion worth to the association. Benchmarking data from other similar organisation will enable the organisation to understand it capabilities compare to its peers and competitors once the CMM is completed (Pironti, 2010).

Maturity Level	General Description	Control Summary	Key Features
5	Optimal, optimizing and business-aligned	• Included in audit and assessment cycles • Control metrics measured and monitored • Developed and utilized process metrics • Complete control quality feedback loop	• Tracked control information and status • Aligned with business processes • Very low associated residual risk level • Meeting or exceeding business requirements
4	Managed, controlled and predictable	• Controls audited and tested for compliance • Defined metrics and thresholds • Standards in place and followed • Operates within recognized processes • Training and awareness complete	• Efficiently operated within formal processes • Embedded in IT processes • Business requirements considered • Low associated residual risk level • Good/excellent effectiveness
3	Proactive, defined and implemented	• Owners trained to operate control • Evenly implemented and monitored • Documented in control catalog • Documented standards • Regular assessment of control	• Good/excellent efficiency • Becoming embedded in IT processes • Widely known and published status of control • Moderate associated residual risk • Effectiveness in an acceptable range
2	Repeatable, reactive and best effort	• Ownership assigned to role, person or process • Implemented inconsistently across organization • Documented via policies and guidelines • Haphazard assessment and/or audit	• Mediocre/fair efficiency • Status usually known by a few • Moderate to high associated residual risk • Effectiveness based on individual effort/expertise
1	Initial, undefined and *ad hoc*	• Not officially assigned to role, person or process • Partially implemented • Not well documented • Not monitored or assessed	• Poor efficiency • Questionable ownership • Vague status • High associated residual risk • Generally unknown effectiveness
0	Intent and not identified	• Control not implemented • Unknown presence of control	• Control not officially in place • Unidentified requirements • Associated risk level assumed to be very high

Figure 2.6: Information Security Management Strategy (Pironti, 2010)

2.3.5 PHASE V – IMPLEMENTATION AND OPERATION

Firstly, in the implementation and operation phase, global consideration need to be put into consideration because threats and risks can vary based on geography so as to be able to understand the socioeconomic data for the regions which the organisation operate to be able to understand the cultural and economic considerations that can impact on strategy. Secondly, compliance and risk need to put into consideration. Thirdly, consequence management needs to be invoked whenever the intended group or organisation does not conform to information security management policies and requirements. Fourthly, board oversight and reporting is very key and is a part of the operational model for information security management strategy to ensure business alignment and also checkmate the organisation in case of defiant. Fifthly, adequate communication needs to be ensured between information security management group and supporting business functions. Finally, social mindfulness should be strengthened in regards to data security exercises are seen inside of the association by changing the centre from security to hazard administration (Pironti, 2010).

2.4 BUILDING EFFECTIVE INFORMATION SECURITY STRATEGY

There has been growing concerns for organisations on the need for effective governance on information security as a result of reliance on technology especially the internet, new regulations from the government and rapid globalisation to protect data. Increasing rate of financial loss and reputational damage as a result of masses data breaches in various companies have made the business executives realise the need for effective information security strategy to protect organisational data. Over the years, information security strategy which places emphasis on using technology rather than people through which breaches occur to design effective security strategy. This approach makes security operate independently of the business which results in security policies and budgets not reflecting the needs of the enterprise. Security is said to be reactive in such an environment, investments in security are driven by short terms priorities rather than long-term strategy and security does not receive management or executives buy in. Effective information security strategy should not involve only technology but also organisation integration and social alignment mechanism (Kayworth and Whitten, 2012). To establish effective information security strategy a gap assessment of organisation current state and the desired state is required, the evaluation is conducted against industry standard such as ISO 27001. Definition of vision, mission, strategy and initiatives is required to enhance the existing information security program (Evans, 2015).

2.4.1 OBJECTIVES OF INFORMATION SECURITY STRATEGY

According to Kayworth and Whitten (2012), the three objectives of information security strategy are balancing the need to secure information assets against the need to enable business, ensuring compliance and maintaining cultural fit.

2.4.1.1 BALANCING INFORMATION SECURITY AND BUSINESS

One of the major challenge faced by management is balancing information security with business; effective information security strategy should be driven by business. The firm should determine the acceptable levels of risk, not the security functions and business should also ensure that in designing the information security strategy the peculiarity of the organisation is taken into consideration (Kayworth and Whitten, 2012). Organisation needs to understand its environment which information systems operate so that information security strategy can address the actual and potential problem. Business need to come first and the strategy must perfume the following functions (i) protects the organisation ability to functions (ii) enables the safe running of the organisation information assets which can be application, network or

systems (iii) protects the information/data the organisation collects and uses this should include data in the state of rest and data in motion and (iv) protects the organisation information assets (Whitman and Mattord, 2011). Business aligned security approach is the key element of business strategy as an organisation requires security practices by embedding information security strategy into the enterprises (Istikoma, Fakhri, Qurat-ul-Ain and Ibrahim, 2015).

2.4.1.2 ENSURING COMPLIANCE

The information security strategy should be designed in such a way that it complies with numbers of regulatory requirement and industry standards like PCI DSS and ISO 27001 (Kayworth and Whitten, 2012). Technology solution is not sufficient to ensure compliance, management control such as policies, procedure and enforcement in addition to technical control has to be put in place (Chen, Ramamurthy, Wen, 2012).

2.4.1.3 MAINTAINING CULTURAL FIT

The third objective of effective information security strategy is to ensure that the information security culture and values reflect the organisational culture (Kayworth and Whitten, 2012). According to Thomson, Solms and Louw (2006), to ensure the integration of organisation culture, security should form part of employees' routine activities. An information security needs to be incorporated into day to activities of an organisation to make it the organisational culture. An organisation with an information security-aware culture is less prone to information security risk as the employees are very much aware of what to do to protect the organisation (Da Veiga and Eloff, 2010). According to Alhogail and Mirza (2014), information security culture is defined as manner at which things are done to ensure that IT assets are well protected.

2.4.2 STRATEGY FOR ACHIVEING INFORMATION SECURITY OBJECTIVES

Effective information security strategy will assist an organisation to achieve the three objectives as explained above which enables the security functions to be strategically focused, business driven and alignment with organisation strategy. The following three risk management mechanism are the strategies to achieve the above objectives (i) organisational integration (ii) social alignment and (iii) technical competence as illustrated in figure 2.5 below: (Kayworth and Whitten, 2012).

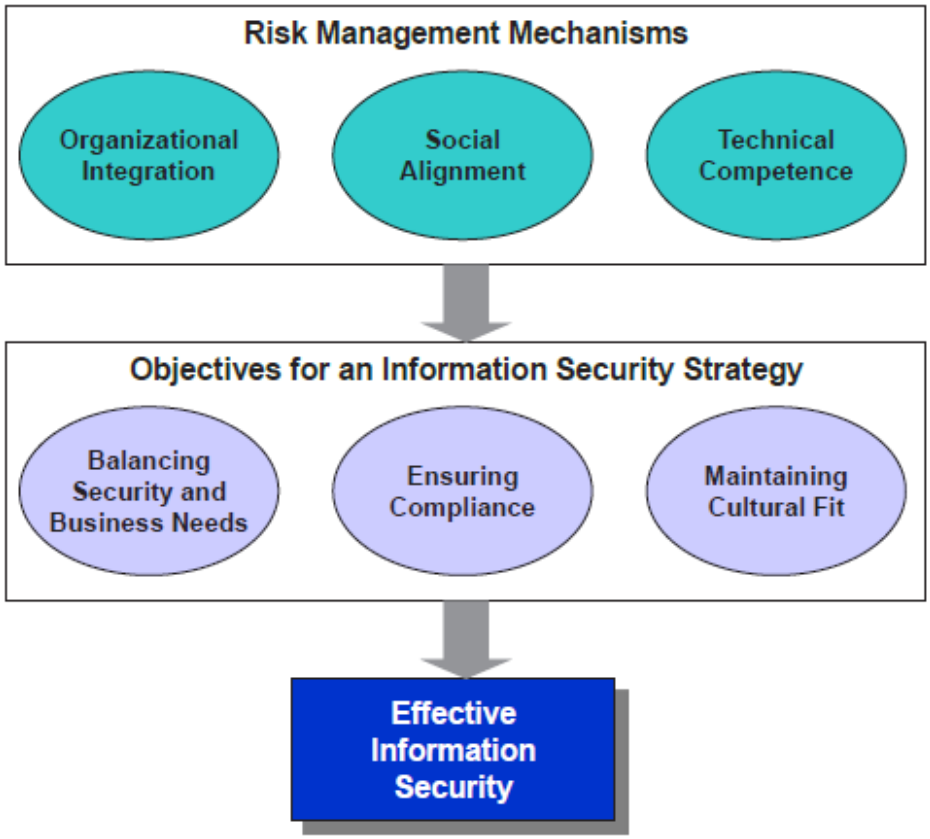

Figure 2.7: A Strategy for Effective Information Security (Kayworth and Whitten, 2012)

From the diagram above, technology is one of the strategies to achieve effective information security strategy, organisation and social alignment is equally important.

2.4.2.1 ORGANISATION INTEGRATION

The nine organisation integration mechanism are explained in figure 2.6 below. The mechanism can be formal organisation structure or coordinating mechanism. In the formal organisation structure, there must be a formal information security unit headed by chief information security officer (CISO) saddle with the overall responsibility of information security governance and reporting directly to the executives and internal audit group whose responsibility is to conduct an independent assessments of information security controls and policies in place. The internal control group is to ensure the effectiveness of all the controls and policies in place and convey results to management. The coordinating mechanism which is further broken down coordinating structures and processes which are further explained in the figure below (Kayworth and Whitten, 2012).

Mechanism	Description	Purpose
Formal Organizational Structures		
Information security organization	A formal organizational unit within the larger enterprise whose mission is to secure the firm's information assets.	To develop and deploy corporate standards and policies governing corporate-wide information security.
Information security executive	Senior-level security executive with leadership responsibility over the information security function.	To facilitate strategic alignment between business and security objectives. To drive the strategic agenda for information security.
Internal audit function	A formal organizational unit that operates independently from the information security function.	To conduct independent assessment of information security controls and policies and to report audit results to senior management.
Coordinating Structures		
Information security steering committee	A cross-functional committee comprised of information security executives and managers from the firm's various business units.	To facilitate communication of strategic business needs, plans, and funding priorities between the business and the information security function.
Information security liaisons	Information security specialists who work in a matrix format with responsibility both to business units and to the corporate information security function.	To represent the interests of the corporate security function by assisting business units in the areas of risk assessment and providing security consulting consistent with corporate security policies.
Separation of security governance from operations	Those responsible for developing security policies maintain operational independence from those responsible for implementation of policy.	To maintain independence between policy makers and implementation personnel and to keep policy makers from being distracted with implementation details.
Coordinating Processes		
Top-down security	Detailed security operating procedures are derived in a top-down fashion from high-level business requirements.	To ensure that detailed security standards and technologies are linked to business requirements.
Information security embedded within key organizational processes	Information security becomes a core element of certain business processes like software development and new product development.	To integrate security into new products, services, and software systems upfront rather than after the fact.
Flexible application of uniform standards	Adhering to uniform security policies across the organization and at the same time allowing for some flexibility in how such standards are deployed.	To allow security policies to be slightly customized to different cultural and geographic contexts.

Figure 2.8: The Nine Integration Mechanism (Kayworth and Whitten, 2012)

2.4.2.2 SOCIAL ALIGNMENT

To ensure motivation of employees for alignment and compliance with various controls and policies of information security, it is crucial to promote cultural awareness. This alignment mechanism can be categorised as cultural and leadership which is further explained in the four social alignment mechanism in figure 2.7 below (Kayworth and Whitten, 2012).

Mechanism	Description	Purpose
Cultural		
Security awareness programs	Organizationally sponsored security awareness, training, and education programs.	To increase the overall awareness of information security and to improve compliance-related behaviors.
Informal networks	Information security personnel engage in boundary-spanning activities to develop close informal relationships with key stakeholders both internally (e.g., IT audit) and externally (e.g., security vendors).	To enhance the level of collaboration between information security and other key stakeholder groups. To improve knowledge sharing on security-related issues among organizational constituents.
Information security mentoring	The practice of providing informal consulting and advisory services to other areas of the company.	To create greater security awareness and buy-in and enhance the likelihood of organizational members seeking advice on security-related issues.
Leadership		
Executive commitment	Senior management actively supports information security as a vital enterprise-wide function.	To establish strong organizational values regarding the importance of information security.

Figure 2.9: Four Social Alignment Mechanism

2.4.2.3 TECHNICAL COMPETENCE

Effective information security does not only require investment in technology as sophisticated technology does not necessarily secure an information asset, but it is also necessary for an organisation to invest in people to ensure competence on the various security tools acquired (Alhogail and Mirza, 2014).

2.4.3 GUIDELINES FOR INFORMATION SECURITY MANAGEMENT

In order to achieve the objectives information security strategy as described above, the following are the guidelines for information security management: (i) determine the appropriate balance between enabling the business and protection information assets; (ii) use a balanced approach to achieving information systems security; (iii) implement formal structures to achieve security objectives; (iv) complements formal structures with coordinating

mechanism and (v) recognise the importance of the social environment. These are explained in the table below (Kayworth and Whitten, 2012).

Guidelines	Description
Determine The Appropriate Balance Between Enabling The Business And Protection Information Assets	The information security manager should consider the culture, compliance requirement and risk appetite of an organisation to ensure the balance between business and information security
Use a balance approach to achieving information systems security	Organisation should consider applying both technology and business integration with social alignment mechanism in order to ensure alignment of security and business
Implement formal structures to achieve security objectives	Organisation should have a security functional unit headed by management which can be CISO and supported by internal audit function to help facilitate organisational integration needed for security objectives
Complements formal structures with coordinating mechanism	Formal structures need to complemented by both coordinating structures and coordinating process as explained in the objectives of security objectives
Recognise the importance of the social environment	Awareness programmes need to be set up for members of staff to understand the importance of information security. This can be driven by the security leader in form of mentoring and interaction with various functions in the organisation

Table 2.3: Guidelines for Information Security Management (Kayworth and Whitten, 2012).

2.5 BENEFITS OF EFFECTIVE INFORMATION SECURITY STRATEGY

According to Evans (2015), information security strategy has the following benefits (i) allows management and employees to be able to prioritise information risk before it crystalize and be able to manage it well. This positions an organisation to mitigate, transfer, accept or avoid the information risk related to people, processes and technology, (ii) it helps organisation protect the confidentiality, integrity and availability of information, (iii) it enables an organisation to have competitive advantage (iv) it allows the organisation to comply with industry standard (v) it allows the organisation to be able to respond and contain security incidence thereby sustaining the organisational reputation and supporting commitment to various stakeholders.

2.6 CONSEQUENCE OF INEFFECTIVE INFORMATION SECURITY STRATEGY

According to Privacy Technical Assistance Centre (PTAC) (2011), advancements in information technology (IT) have resulted in increased concerns about the risks to information associated with ineffective information security practices. These risks are vulnerability to viruses, malware, attacks and compromise of network systems and services. Inadequate security practices result in compromised confidentiality, integrity, and availability of the data due to unauthorised access. A technical threat such as non-existence security architecture, poor configuration management can lead network exploitation and loss of customers' critical data such as personally identifiable information, malicious software, hacking. Non-technical threats to information systems such as insider threats, poor password policy, insufficient backup and recovery, social engineering can lead to stolen customers' confidential data, access to most sensitive information and risk associated with data breach.

2.7 ELECTRONICS FRAUD (E-FRAUD)

According to Behdad, Barone, French and Bennamoun (2012), fraud is when one person obtains an unjust advantage over another using false leading representation. E-fraud is when one person use technology (network intrusion, email spam, online credit card fraud, telecommunication and hacking tools) to take an unjust advantage over another. According to the US Department of Justice as cited in Neff (2014), e-Fraud is as an extortion plan that uses one or more segments of the web -, for example, chats, email, message boards, or Web to display false requesting to forthcoming casualties, to lead fake exchanges, or to transmit the returns of misrepresentation to money related foundations or to other associated with the plan. No matter the size of financial institutions, if customers are offered electronic access such as

online banking they are faced with e-fraud risk. Hackers always seek out and uncover weaknesses in the bank's fraud defences (ACI, 2014).

According to Nigerian Electronic Fraud Forum (NEFF, 2014), electronics fraud is the use of information technology to commit a crime for personal gain which is usually financial. Electronic fraud can be Card Fraud, which involves the fraudster stealing the card details to perpetuate fraud or phishing and identity which has to do with sending of fake e-mail or web links to unsuspecting victims with the hope of stealing sensitive information like password, account details, card details or infect the computer with a virus.

2.7.1 PREVENTION OF E-FRAUD

According to ACI (2014), preventing of e-fraud requires a layered and risk-based approach because cybercrime and e-fraud is an evolving threat. Some of these threats are malware, social engineering, denial of service/distributed denial of service, insider threat, exploitation of a weaker online platform-compromise of one site; malicious users can use similar techniques may gain access to credentials of other vulnerable websites. Adoptable control practices to prevent e-fraud are public/customer awareness on fraudsters' activities; strict adherence to internal policies and procedures; adequate funding of collaborative forum for tackling electronic fraud; implementation of limits on all electronic platforms to minimize exposure; enforcing second factor authentication on all financial channels; authentication of all card transactions; embedding information security to systems development life cycle; training of staff on emerging threats; implementation of electronic fraud risk management; transaction monitoring; effective know your customer (KYC) process in place; compliance with regulatory standard; adherence to information security best practices such as ISO 27001; PCI DSS (NEFF, 2014).

According to NEFF (2014), the following considerations should be considered by Nigerian financial institutions in order to mitigate e-fraud risk (i) implementation of fraud monitoring solutions; (ii) overhauling IT Security; (iii) paying attention to insider threats (iv) intensifying anti-fraud awareness program and (v) Implementing a formidable e-fraud detection-prosecution process.

2.7.2 FRAUD MONITORING SOLUTIONS

These are technology solutions that detect suspicious transactions and behaviours. Transaction monitoring is very effective in fighting against fraud at the application level as fraudster are not comfortable whenever they realise that their activities are monitored. This solution can detect, analyse and prevent fraudulent transactions on e-payment platforms. The financial institution should ensure that a dedicated unit is set up to ensure that the solution is fully optimised and also ensure that the solution is not deployed to meet regulatory requirement only but to ensure optimised utilisation (NEFF, 2014).

2.7.3 OVERHAULING IT SECURITY

The IT security posture of the financial institution needs to be improved upon to ensure adequate control/countermeasure is in place. This can be achieved with a robust information security framework which is in line with best practice. Apart from accreditation based on this framework, the bank should also ensure adequate cybersecurity control (such as the implementation of strong authentication control, robust antivirus programme, network segmentation to isolate critical systems and prevent unauthorised access) is in place to prevent the advance attack (NEFF, 2014).

2.7.4 COMBATING INTERNAL THREAT

According to Cappelli, Moore and Trzeciak (2012), a malicious insider threat is a person (current employee or former employee, contractors) that has authorised to company's network, systems or data and misused the access in such a way that the confidentiality, integrity and availability of information asset are in question. They explained the best practices for the prevention and detection of insider threats which are: (i) considering threats from insiders and business partners in enterprise-wide risk assessments (ii) clearly document and consistently enforce policies and controls (iii) periodic information security awareness for all employees (iv) monitoring and responding to suspicious or disruptive behaviour, beginning with hiring process (v) anticipating and managing negative workplace issues (vi) track and secure the physical environment (vii) Implement strict password- and account management policies and practices (viii) enforce separation of duties and least privilege (ix) consider threats in the system development life cycle (x) Use extra caution with systems administrators and technical or privileged users (xi) implement systems change control (xii) log, monitor, and audit every employee on electronics platform (xiv) Deactivate computer access immediately after

termination (xv) Implement secure backup and recovery process and (xvi) develop an insider incidence response plan.

Disgruntled employees that are knowledgeable in IT can exploit the weakness in e-payment solution or internal control to commit e-fraud (NEFF, 2014).

2.7.5 INTENSIFY ANTI-FRAUD AWARENESS PROGRAM

Most e-fraud cases are aided by social engineering techniques – non technical method of hacking into systems by playing on human psychology. The best way to combat social engineering is to assist people to identify and respond to threats –through a massive awareness campaign (NEFF, 2014).

2.7.6 IMPLEMENTING A FORMIDABLE E-FRAUD DETECTION-PROSECUTION PROCESS

In order to prevent e-fraud in Nigerian financial institution, it expedient for Nigerian banks to have a centralised fraud monitoring team (all Nigerians banks should be represented). It will ensure timely detection and prevention of fraudulent transactions. Leadership of all Nigerian banks with Economic and Financial Crime Commission (EFCC) and CBN should also pass a bill aid the prosecution of such crimes – this bill was later passed in 2015 (NEFF, 2014). According to Cybercrimes Act (2015), cybercrime act provides an effective regulatory framework for the prevention, detection, prosecution of cybercrimes in Nigeria and also ensures the protection of critical national information infrastructure and promotes cybersecurity and the protection of computer systems and network, intellectual property and privacy rights.

2.8 THEORETICAL FRAMEWORK

2.8.1 CYBERSECURITY FRAMEWORK

The Framework gives a typical scientific classification and instrument for associations to depict their present cybersecurity stance; portray their objective state for cybersecurity; distinguish and organize open doors for development inside of the connection of a ceaseless and repeatable procedure; evaluate progress toward the objective state and convey among interior and outside partners about cybersecurity hazard. It is a risk based approach to deal with preventing so as to secure information, distinguishing, and reacting to attacks and comprises three parts which are the framework core, framework implementation tiers and framework profiles (NIST, 2014).

2.8.1.1 The Framework Core

This consists of five concurrent and continuous functions which are Identify, Protect, Detect, Respond, Recover which provide a high-level, strategic view of the lifecycle of an organisation's management of cybersecurity risk and core four elements which are functions, categories, subcategories, and informative reference as explained in the figure below.

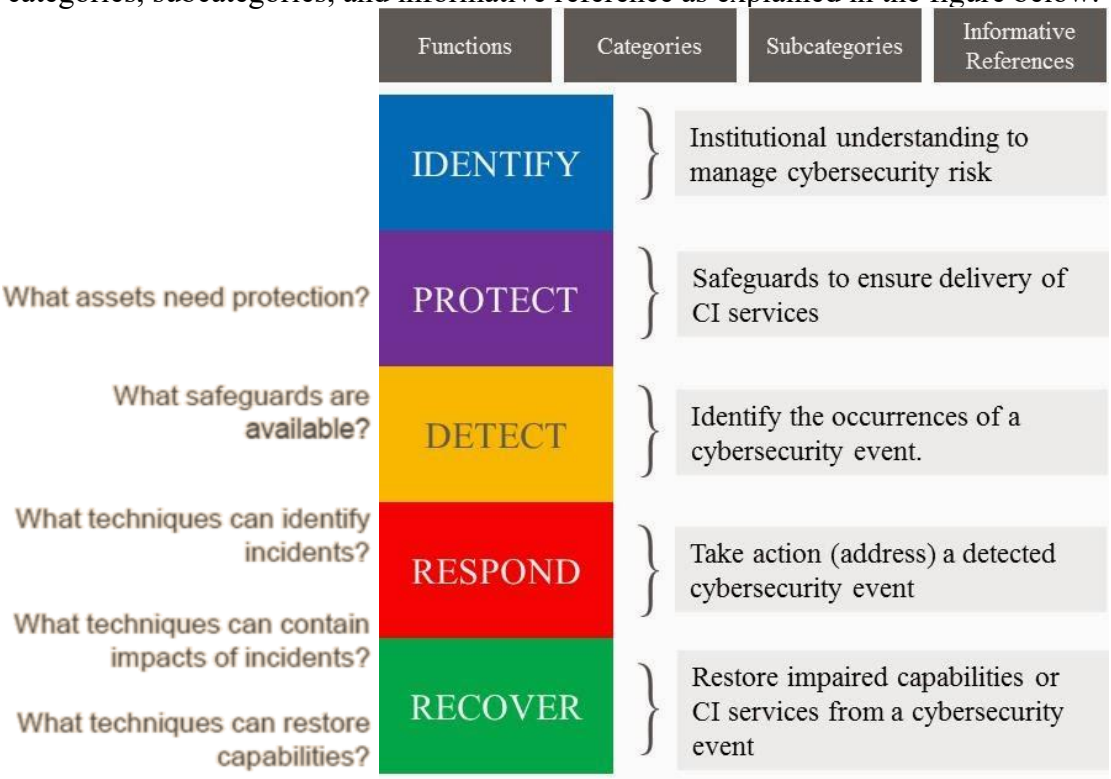

Figure 2.10: Cybersecurity Core Framework explained

the core principle is the fundamental of how an organisation should view its cybersecurity practices which are asset identification; procedures to protect the organisation information asset; personnel to identify cybersecurity incidences; procedures to respond to security incidence and recover from cybersecurity breaches whenever it occurs. Retrieved February, 29, 2016 from https://corpgov.law.harvard.edu/2014/08/25/understanding-and-implementing-the-nist-cybersecurity-framework/ . The core elements are explained below:

Functions: These are high level cybersecurity activities namely identify; protect; detect; respond and recover as further illustrated in the figure below. The *identify* function has to do with the development of business context in order to manage risk to information asset thereby enables the organisation to be able to analyse and assess cyber threats on IT assets using appropriate tools and methods. *Protect* function ensures the development and implementation of appropriate controls to ensure protection of information assets. *Detect* function ensures that

there is adequate practice such as audit logs, penetration testing, vulnerability management etc. to identify the occurrence of cybersecurity events. *Respond* has to do with the appropriate action such as maintaining incidence response plan regarding identified cybersecurity events. *Recover* has to do with plans for resilience and to restore services that were impaired during cybersecurity events (NIST, 2014).

Categories: These are the subdivision of the functions group into specific activities to be carried out such as asset identification and access control.

Subcategories: These further divides the category section into more detailed technical and management activities to be carried out to ensure adequate cybersecurity in place.

Informative Reference: These are specific standards, guidelines, practices to achieve the objectives of the subcategories such standards are COBIT, PCI DSS and ISO 27001.

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Figure 2.11: Function and Category Unique Identifiers (NIST, 2014)

2.8.1.2 FRAMEWORK IMPLEMENTATION TIERS

These provide context on how a company views cybersecurity risk and the processes in place to manage that risk. Tiers describe the maturity of an organisation's cybersecurity risk management practices which are categorised as Partial, Risk-Informed, Repeatable and Adaptive. (NIST, 2014). In Tier 1 (Partial), the organisation cybersecurity management practice is not defined; there is no adequate awareness on cybersecurity risk and coordination approach in managing risk is not established. In Tier 2 (Risk-Informed), cybersecurity risk management policy is approved by the Directorate but not established as organisational-wide policy. In Tier 3 (Repeatable), there is cybersecurity procedures/policies which are updated regularly based on business requirements, changing threat and technology landscape. Cybersecurity personnel are well equipped, and organisation understands the dependencies between business partners to collaborate and make an informed decision which is risk-based. In Tier 4 (Adaptive), cybersecurity practices are based on the lesson learned and predictive indicators derived from previous and current activities. There is an organisational-wide policy, procedures and processes that are risk based as cybersecurity risk management is part of the organisation structure. The organisation shares their cybersecurity risk management experience with partners (NIST, 2014).

2.8.1.3 FRAMEWORK PROFILES

It is the alignment of the functions, categories and subcategories with the business requirements, risk tolerance, and resources of the company. The Profile can be portrayed as the arrangement of measures, rules, and practices to the Framework Core in a particular execution situation. Profiles can be utilized to distinguish open doors for comparing so as to enhance cybersecurity stance a "Present" Profile (the "as may be" state) with an "Objective" Profile (the "to be" state). To add to a Profile, an association can audit the greater part of the Categories and Subcategories and, taking into account business drivers and a danger evaluation, figure out which are most imperative; they can include Categories and Subcategories as expected to address the organisation's risks (NIST, 2014).

Having set up the Current and Target Profiles, an organization can distinguish holes between the two and set up a guide for regions that the organization needs to fortify keeping in mind the end goal to advance toward its objective state (Shen, 2014).

2.8.1.4 BENEFITS OF CYBERSECURITY FRAMEWORK

According to Shen (2014), companies can use the framework to determine their existing cybersecurity posture whether it is adequate or not, if not develop one from scratch. They can set objectives for cybersecurity that are in agreement with business objectives to prioritize opportunities for improvement/establish a plan for improving or maintaining their cybersecurity. The framework is very important to help the management understand their company's security practices thereby enable them see how their company's cybersecurity practices align with the framework's standards, understand where the company's vulnerabilities, and determine if they are doing enough.

The framework provides the standardization approach to addressing the approach to cybersecurity concerns. It helps the organisation to collaborate by sharing cybersecurity best practices and lessons learned. Organisation using the framework will be able to demonstrate due care in cybersecurity incidence by providing the stakeholders with information on the posture. The framework enables the security auditors to be able to evaluate the organisation security posture in one standard format which eliminates the needs for various security compliance document. It provides an opportunity for the organisation to better understand the risk imposed by their supply chains which enable the organisation to spend security budgets wisely. All these benefits are illustrated in the figure 2.7 below. Retrieved February, 29, 2016 from https://corpgov.law.harvard.edu/2014/08/25/understanding-and-implementing-the-nist-cybersecurity-framework/

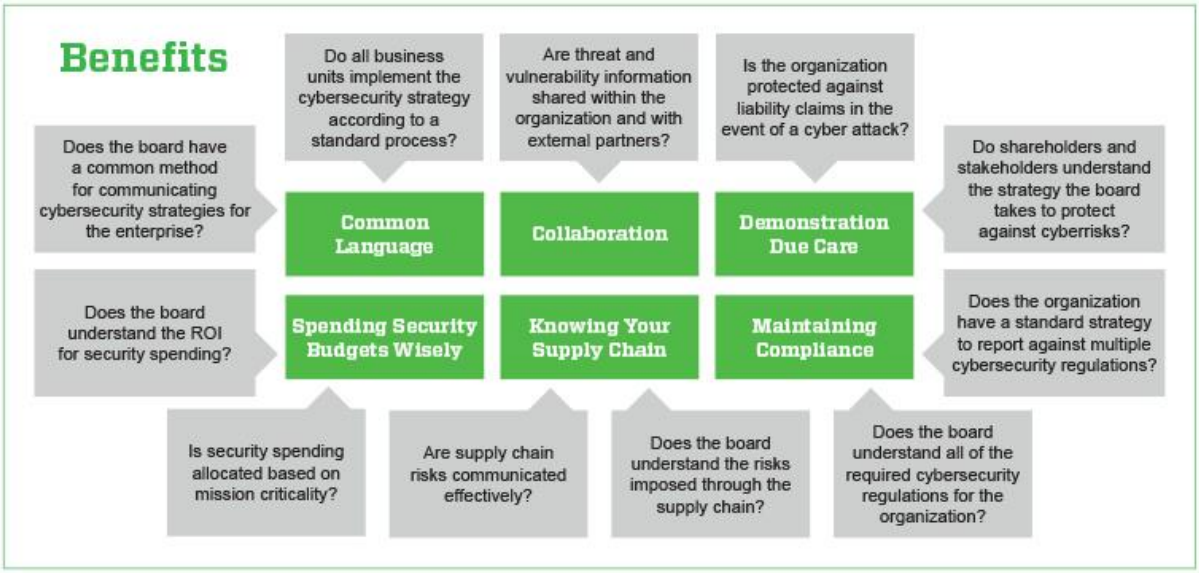

Figure 2.12: Benefits of Cybersecurity Framework

2.8.1.5 STEPS IN ESTABLISHING OR IMPROVING CYBERSECURITY PROGRAM

According to NIST (2014), the following are the steps in establishing or improving cybersecurity program:

1. Prioritize and Scope—Requests that organisations scope and prioritize business/mission objectives and high-level organisational priorities. This information allows organisations to make strategic decisions regarding the scope of systems and assets that support the selected sectors of activity or processes within the organisation.
2. Orient—Provides organisations an opportunity to identify threats to, and vulnerabilities of, systems identified in the Prioritize and Scope step.
3. Create a Current Profile—identifies the requirement to define the current state of the organisation's cybersecurity program by establishing a current state profile.
4. Conduct a Risk Assessment—Allows organisations to conduct a risk assessment using their currently accepted methodology.
5. Create a Target Profile—Allows organisations to develop a risk-informed target state profile. The target state profile focuses on the evaluation of the Framework Categories and Subcategories describing the organisation's desired cybersecurity outcomes.
6. Determine, Analyse, and Prioritize Gaps—Organisations carry out a security assessment to determine the current status to improve on the current posture. The gaps are recognized by overlaying the present state profile with the objective state profile.
7. Implement Action Plan—After the gaps are identified and prioritized, the required actions are taken to close the gaps and work toward obtaining the target state

2.8.1.6 CRITICISM OF CYBERSECURITY FRAMEWORK

The framework has no enforcement authority; the organisation can use their discretion whether or not comply with the framework (Lei, 2014). The framework does not clearly define how to protect critical infrastructure it only references various standards. Retrieved March 8, 2016 from http://www.digitalcrazytown.com/2014/08/nist-cybersecurity-framework-is-good.html. Implementing the framework is not straightforward and does not take into consideration threats unique to an organisation. Retrieved March 8, 2016 from

http://searchsecurity.techtarget.com/news/2240214505/Final-version-of-NIST-cybersecurity-framework-draws-mixed-reviews

2.8.2 COBIT 5 FRAMEWORK FOR INFORMATION SECURITY

According to ISACA (2012), COBIT 5 framework is a detailed framework for the management and governance of enterprise. The framework enables the organisation derives optimal value from IT. The major drivers for the development of the framework are

1. Gives the stakeholders a sense of belonging on what they expect from IT and what to be done in order ensure value from IT
2. Address the dependency of organisation success on external IT parties and business
3. Helps an organisation in the management of information effectively
4. IT is seen as an integral part of the business
5. It provides guidance on innovation and emergence technology
6. It covers the full end-to-end of business and IT functional responsibilities which lead to effective governance and management of enterprise IT
7. Get better control over user activities on the operation of IT
8. Aligns with other IT and information security industry
9. Enable organisation to achieve value creation on the use of enterprise IT, users satisfaction on IT services, compliance with industry standard, improvement in relationship between business and IT objectives

The framework covers the lifecycle of governance, strategic and tactical management of IT domain (De Haes, Van and Debreceny, 2013).

The product family for the framework includes:

1. COBIT 5 (framework)
2. COBIT 5 enablers guides which described the governance and management in detail which are enabling processes, enabling information and other enabler guides
3. COBIT 5 professional framework which include:
    a. COBIT 5 Implementation
    b. COBIT 5 for Information Security
    c. COBIT 5 for Assurance
    d. COBIT 5 for Risk
    e. Other professionals guides

This study focus is on COBIT 5 for Information Security framework (ISACA, 2015).

COBIT 5 for information security framework provides a comprehensive ways of ensuring reasonable and appropriate control for information resources. The major drivers for the development for COBIT 5 for information security are to (i) describe information security within the context of organisation (ii) the need for an enterprise to maintain information risk within business acceptable level to ensure the confidentiality, integrity and availability of information resources by complying with industry standard as relevant to the organisation (iii) the for stakeholders to understand the industry standard and how to use them together and (iv) the need to link all other ISACA associated framework, research and guidance.

The framework is based on five guiding principle as illustrated in the figure below:

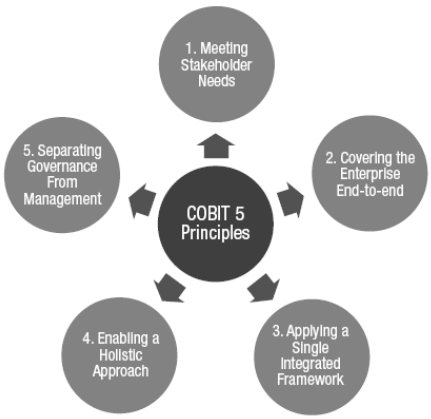

Figure 2.13: COBIT 5 Framework for Information Security Principle (ISACA, 2012)

2.8.2.1 *COBIT 5 Framework for Information Security 5 Guiding Principles*

These five guiding principles are: (i) meeting stakeholder needs: this is very crucial to know the current or future states of the security process, systems and policies. Their input is required to ensure that the outcomes align with the requirements. It is very important in IT security project planning and risk management. Successful stakeholder analysis results in benefit maximization, risk minimization and resources optimization this is further illustrated in figure 2.14 below

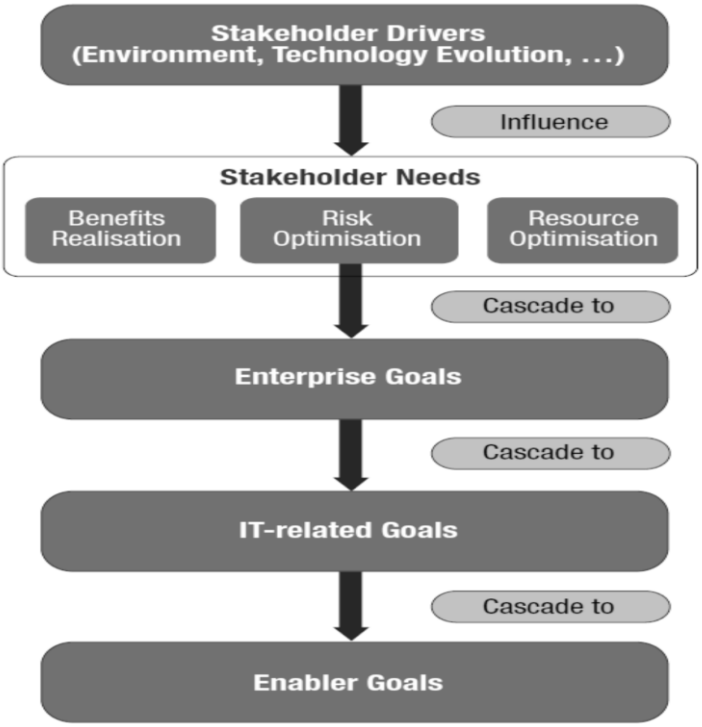

Figure 2.14: COBIT 5 Goals Cascade- Stakeholder Drivers (ISACA, 2012)

(ii) covering the enterprise end to end: the framework covers all stakeholders, functions and processes and procedures that are relevant to information security, security review and assurance should be part of all business process and IT operational activities (iii) applying a single intended framework: application of security controls is often a point-and-shoot activity. It is a typical practice for some organisation to alter particular issues without venturing back and applying arrangements and controls that affect numerous vulnerabilities in network, systems or application. Designing a complete framework includes all aspects of data storage, flow, and processing, providing a foundation for more efficient control implementation. Creation of control matrix is very crucial as shown in the Appendix 1 (iv) enabling a holistic approach: in order to support development of an integrated framework, IT security controls should be seen as a set of related components not as a set of silos which are driven by 7 enablers described in the next section (v) separating governance from management: governance defines the objectives while the management is responsible for the operational activities to meet the technology and information security goals (ISACA,2012).

2.8.2.2 *COBIT 5 Framework for Information Security Enablers*

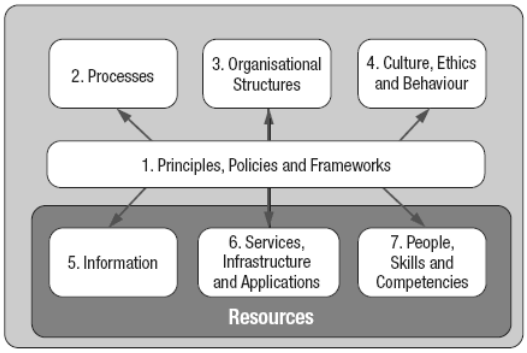

Figure 2.15: COBIT 5 Enablers (ISACA, 2012)

COBIT 5 frameworks for information security enablers are illustrated in the figure 3 above. The COBIT 5 enablers are described as follow: (i) Information Security Principles, Policies and Frameworks provide means to integrate all enablers to have a secure operational success. ISO 27001 is one of the best- known standard that provides requirements for an information security management system (ISMS). An ISMS is a systematic approach to managing sensitive company information so that it remains secure. It includes people, processes and IT systems by applying a risk management process; (ii) Processes including information security-specific details; (iii) Information security-specific organisational structures is designed to monitor and reach strategic and operational objectives. Leaders (decision makers) from each level are typically stakeholders in business processes and expected outcomes; (iv) Culture, Ethics and Behaviour(factors determining the success of information security governance and management) is very crucial as these change the employees see their working world and try to ensure secure workplace; (v) Information this should be well protected because of its criticality to business operations and should be made available whenever when and where needed and IT delivers ; (vi) Services Infrastructure and Applications. Retrieved February 25, 2016 from http://www.techrepublic.com/blog/it-security/cobit-5-for-information-security-the-underlying-principles/

2.8.2.3 Benefits of *COBIT 5 Framework for Information Security*

According to ISACA publication COBIT 5 for information security (2012), the benefits of the framework are: (i) to reduce complexity and increased cost-effectiveness as a result of improved and easier integration of information security standards; (ii) to increase user satisfaction with IT security arrangements and outcomes; (iii) to improve integration of IT security controls in the enterprise; (iv) to enhance informed risk decisions and risk awareness;

(v) to improved prevention, detection and recovery in a case of fraud; (vi) to reduce impact of security incidents such as hacking and e-fraud; (vii) to enhance support for innovation and competitiveness (viii) To improve management of costs related to the information security function and (ix) for better understanding of information security

2.8.2.4 CRITICISM OF COBIT 5

According to Zhang and Le (2013), COBIT is difficult to implement as it requires great effort to learn and understand the framework because of the large numbers of IT processes and control objectives. The COBIT guidelines do not provide specific details of utilization. According to De Haes et al (2013), COBIT 5 is a complex set of standard.

2.8.3 PCI DSS FRAMEWORK

To prevent escalating cards fraud which is a form of e-fraud, five organisation namely MasterCard Worldwide, America Express, Discover Financial Services, JCB International, and Visa Inc. formulated the PCI DSS to assist all cards Industries (PCI, 2015). According to Calder and Williams (2014), the framework applies to anywhere cardholder information resides which can be hard drives, removable storage devices, back-up media and printed materials which apply to the process, people and technology such as systems, servers, applications or other technologies that are connected to cardholder data environment. The standard mitigates financial risks associated with payment data breaches.

PCI DSS is a global standard developed to enhance protection of cardholder and facilitate the broad adoption of consistent data security. It provides both operational and technical requirements to protect customers' account data. The standard specifies twelve requirements for compliance which are explained in the subsections below. This compliance is organised into six control objectives as shown in Table 2 below. Retrieved January 17, 2016 from https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-1.pdf.

Control Objectives	**PCI DSS Requirements**
Build and Maintain a Secure Network	1. Introduce and keep up a firewall design to ensure cardholder information

	2. Try not to utilize merchant supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data
	4. Encode transmission of cardholder information crosswise over open and public systems
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs
	6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Confine access to cardholder information by business need-to-know
	8. Identify and authenticate access to system components
	9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all forms of access to network resources and cardholder data
	11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Keep up a strategy that addresses information security for all staff

Table 2.4: PCI DSS Requirement

2.8.3.1 INTRODUCE AND KEEP UP A FIREWALL DESIGN

According to PCI (2015), to ensure adequate establishment and configuration of firewall and router, there should be a formal process for approving and testing all network connections and changes to the firewall and router configurations. It means that the change management process must strictly adhere whenever there is the request for the change in the firewall or router configuration. It is required to have detailed network diagram that shows all connection to systems that store sensitive data such as personal account number (PAN), card expiry date, personal identity number (PIN) and card verification value (CVV). The network design should be in such a way that there is a firewall at each internet connection, and there should be a physical or logical network that separates an internal network from other untrusted network

and firewall should be placed in between this zone. The framework requires adequate access control to all network components, disabling of all services, ports and protocols not needed by card systems/network and there should be a proper documentation where insecure protocols are used. To achieve all of these, there will be a need for periodic reviews of router and firewall configuration which can be twice per annum at the minimal.

To protect cardholder data from external attacks such as malware or hacking, it is expedient to disallow direct access to the Internet and systems in such environment. For systems that will require direct internet access such as employees' laptops or desktops, personal firewall software must be installed on such systems (PCI, 2015).

2.8.3.2 PROHIBITION OF DEFAULT VENDOR-SUPPLIED CONFIGURATION

The framework emphasizes on the need to change all vendor-supplied defaults configuration such as passwords, account name and simple network management protocol (SNMP). It also emphasizes the need to develop configuration standards for all systems and such standards must be in line with industry practice such as standards that addresses known vulnerabilities like hardening of systems. All administrative must be done in a secure manner by ensuring encryptions of communication to cardholder systems, and organisation should ensure that their shared hosting providers provide assurance that cardholder data are well protected (PCI, 2015).

2.8.3.3 PROTECT STORED CARDHOLDER DATA

To protect cardholder data in storage, there should be a data retention and disposal policy in place, sensitive authentication data after authorisation such as the track of magnetic stripe – located at the back of the card, CVV, PIN. PAN should be rendered unusable for malicious users that have access to it if there is the need to be stored in any form. Organisation should ensure that all keys used to have access to cardholder data are protected against disclosure and misuse by ensuring adequate standards in key management as informed by best practices (PCI, 2015).

2.8.3.4 ENCRYPT TRANSMISSION OF CARDHOLDER DATA

Transmission of cardholder data over open or public network should be done in a secure manner. PAN should not be sent over end-user messaging technologies such as SMS, email, chat, etc. which is achievable by ensuring that security policies and operational procedures for encrypting transmissions of cardholder data are documented, in use, and communicated to all stakeholders (PCI, 2015).

2.8.3.5 PROTECT ALL SYSTEMS AGAINST MALWARE

To protect systems against malware, it is crucial for all systems to have antivirus install. The antivirus definition must be up to date to guide against known vulnerabilities. Adequate antivirus program should be well maintained and ensure that the antivirus is current, performs periodic scans and generates audit log in order to be able to monitor and virus and malware activity and anti-malware effectiveness (PCI, 2015).

2.8.3.6 DEVELOP AND MAINTAIN SECURE SYSTEMS AND APPLICATIONS

An organisation should ensure that all applications and systems are protected from known vulnerabilities by ensuring that they are adequately patched. The suitable process to identify risk in security should be put in place and software security need to be embedded into system development life cycle. Security is best achieved when it is being planned with the systems. Software coding standard should be in line with industry security standard such Open Web Application Security Program (OWASP) Guide, SANS CWE Top 25, Cert Secure Coding, etc. to protect it from a common vulnerability which can be exploited by hackers (PCI, 2015).

2.8.3.7 RESTRICT ACCESS TO CARDHOLDER DATA

According to PCI (2015), to restrict access to cardholder data by business need to know, access should be limited to staff whose job responsibilities require such access and all access should be denied except there is a business need to know.

2.8.3.8 ASSIGN A UNIQUE ID TO EACH PERSON WITH COMPUTER ACCESS

To ensure adequate accounting user identification and authentication management process needs to be put in place. This helps the organisation to speed up issue resolution and be able to contain the issues whenever malicious intent occurs. These can be ensured by assigning all users unique ID before given access to cardholder data, revoking users access immediately after exiting from the organisation, implementing two factors authentication whenever require and adequate access control (PCI, 2015).

2.8.3.9 RESTRICT PHYSICAL ACCESS TO CARDHOLDER DATA

The following should be put in place in order to ensure adequate physical access control to cardholder data: using appropriate facility entry controls to limit and monitor physical access

to systems in the cardholder data environment such as closed circuit television and restricting access to open network ports; developing a process to easily identify staff from visitors; storing media backups and media securely; appropriately destroying when no longer in use (PCI, 2015).

2.8.3.10 TRACK AND MONITOR ALL ACCESS TO NETWORK RESOURCES

All systems activities need to be logged and monitored continually in order to ensure adequate tracking in the case of fraud or whenever there is need for forensic. PCI emphasizes on the following to achieve adequate tracking and monitoring all access to network resources and cardholder data: implementation of audit trails on users' activities; the audit trail should capture all necessary information such as user identification, event type, date and time, success or failure indication that would be required for forensic; synchronization of all systems time to ensure ease comparing logs from different systems and establishing an exact sequence of event; protection of audit trail from malicious alteration; Reviews of log for security incidence; Retention of audit trail and implementation of policy for the tracking and monitoring of all access to network resources (PCI, 2015).

2.8.3.11 REGULARLY TEST SECURITY SYSTEMS AND PROCESSES

According to Klie (2015), PCI recommends that organisation take an inventory of all the IT assets and business processes and analyse them for vulnerabilities that could expose customers' data. Having identified the vulnerabilities, the next step is to fix them.

There is need for systems to be tested on a periodic basis due to new vulnerabilities being discovered frequently. PCI requires the implementation of process to test for rogue wireless access; implementation of vulnerability management systems to identify weakness in design or threat to systems in order to address them; penetration testing practice to simulate the activities of hacker in order to be able to quantify risk to information asset and come up with controls to mitigate the risk. In order to detect or prevent attack into the network, intrusion-detection and/or intrusion prevention systems are required. This systems signature need to be kept updated and well configured in order to detect or prevent new attacks. PCI also requires the deployment of file-integrity monitoring tools to alert IT security personnel on any unauthorised modification to critical files such as systems executable, application executable, configuration and parameters files (PCI, 2015).

2.8.3.12 MAINTAIN AN INFORMATION SECURITY POLICY

Information security policy is a roadmap for implementing company's information security strategy. Personnel awareness is the key critical success factor for implementing security measures. The policy needs to be established, maintained and disseminated. An organisation needs to carry out a risk assessment at least annually or whenever there is major changes in order to identify threats and vulnerabilities that can impact on the business and also ensures that the information security policy and procedures are clearly defined in security responsibilities for all staff. Personnel's whose jobs' functions relate to information security should be aware of their responsibilities and how to secure the organisation information assets (PCI, 2015).

2.8.3.13 CRITICISM OF PCI DSS

According to Flick (2009), PCI DSS does not require a high-level of security in cardholder data environment. The standard allows self-appraisal for merchants that processes card data which can form the basis of bias of the assessment report. The merchant is required to fill in the self-assessment questionnaire (SAQ) instead of assessment by an approved independent party which can lead to under assessment.

2.9 SUMMARY OF LITERATURE REVIEW

S/N	Themes	Findings	Authors
1	Information Technology & Information Security	The section described how Information technology brought improvement to the management of information. It described how financial institutions leveraged the use of information technology for payments system and the need for information security management in order to mitigate risk against confidentiality, integrity and availability of information assets in financial institution.	Haag and Cummings (2013);Fabian (2003); Matthew *et al* (1999); Zhao *et al* (2013); NeFF (2015); Usman and Shah (2013); Harris (2013); Whitman and Mattord (2012); COBIT (2012); NIST (2014); Klie (2015); ISO 27001 (2013);

2	Information Security Management Strategy	This section identified the steps for developing information security management and how to develop information security management strategy	Ricky and Monique (2014); LeVque (2006); Young and Windsor (2010); Pironti (2010); Whitman (2003)
3	Building Effective Information Security Management Strategy	The section described how effective information security management strategy can mitigate financial loss as a result of the use of technology. It described the objectives of effective information security strategy, strategies achieve these objectives and guidelines to achieve the objectives	Kayworth and Whitten (2012); Evans (2015); Istikoma *et al* (2015); Chen *et al* (2012); Thompon *et al* (2006); Da Veiga and Eloff (2010); Alhogail and Mirza (2014)
4	Benefits of Effective Information Security Strategy	This section explained the benefits of effective information security strategy	Evans (2015)
5	Consequence of Ineffective Information Security Strategy	The section described the consequence of ineffective information security strategy	PTAC (2011)
6	Electronic Fraud	The section described the concept of e-fraud, how to prevent it through effective information security strategy	Behdad *et al* (2012); ACI (2012); NEFF (2014); Cappelli *et al* (2012)
7	Theoretical Framework	The section described the various theoretical framework that can be used to achieve effective information security management strategy and the criticism	NIST (2014); Shen (2014); Lei (2014); ISACA (2012); De Haes (2013); Zhang and

		of each of the framework by various authors	Le (2013); PCI (2015); Klie (2015); Flick (2009)

Table 2.5: Summary of Literature Review

2.10 CONCLUSION

This chapter reviewed relevant literature on information management, information security, information security management strategy, e-fraud, cybersecurity as well as the theoretical framework guiding the study. The next chapter describes the research method and process used in this study.

CHAPTER THREE

3.0 RESEARCH METHODOLOGY

3.1 INTRODUCTION

The objective of this chapter is to report and present the methodology of the study that was conducted. The chapter looks at the research design that was used in addressing the research questions, a description of the sample group the research instruments used and the method of analysis.

3.2 RESEARCH DESIGN

The research design is a survey. It used a qualitative approach that comprised of a group discussion session (much similar to a focus group) of the head of units whose functions are related to the management of information security and interview sections with team leads. The discussion session and the interviews were conducted based on scripts that was prepared by the researcher.

3.3 POPULATION OF STUDY

The target population of the study was 15 senior employees of Enterprise bank in the following division: information technology group; information systems control; IT audit and enterprise risk management. The population was targeted to these categories of staff due to their roles in controls and risk management in the bank. Interviews were conducted to nine senior staff who are the various team leads of different units in the targeted departments. A group discussion was conducted to six senior management of the researcher's organisation.

3.4 SAMPLE AND SAMPLE SIZE

3.4.1 DISCUSSION GROUP

As a result of the research type conducted by the researcher, it was imperative to ensure a careful selection of participants, only very senior management of the researcher's organisation were invited to participate in the session. The profile of participants is given in Table 3.1 below:

S/N	Title/Designation
1	Chief Information Officer
2	Chief Risk Officer
3	Chief Compliance Officer
4	Chief Internal Auditor

5	Chief Information Security Officer
6	Group Head, E-Business

Table 3.1: Profile of Participants

3.4.2 INTERVIEWS

The population of the study is made up of nine team leads (senior staff) whose jobs' responsibility were related to the management of information security in the bank.

3.5 RESEARCH INSTRUMENT

3.5.1 INSTRUMENT USED FOR THE DISCUSSION GROUP

The researcher prepared a list of questions – based on the research questions and the recommended approaches in the literature review, to serve as a script for the discussions.

In addition to the question guide, the researcher encouraged the participants to ask follow-up questions similar to the pattern of questions recommended for action learning sets. The script contained 12 questions

1. Question 1-6 relate to research objective 1
2. Question 7 relate to research objective 2
3. Questions 8 – 10 relate to research objectives 3
4. Questions 11-12 relate to research objective 4

3.5.2 INSTRUMENT USED FOR THE INTERVIEWS

The researcher prepared a question guide to act a script for discussion with the management staff to be interviewed. The questions were related to all the objectives. An in-depth interview is an open-ended, discovery-oriented method to obtain detailed information about a topic from a stakeholder. According to Wallace Foundation (2015), in-depth interviews are a qualitative research method; their goal is to explore in depth a respondent's point of view, experiences, feelings, and perspective on the subject matter. By means of a thorough composed interview guide, the interviewer ensures that the conversation encompasses the topics that are crucial to ask for the sake of the purpose and the issue of the survey (Megafon, 2015). In addition, the in-depth interviews were done using the question guide in Appendix I. The in-depth interview

helped to throw more insight into the research objectives as questions were allowed to flow naturally based on information provided by the respondent. The script contained 18 questions.

1. Questions 1 – 3 relate to research objective 1
2. Question 4 - 12 relate to research objective 2
3. Questions 13 – 16 relate to research objective 3
4. Question 17 - 18 relate to research objective 4

The interviews were conducted during lunch hour and scheduled meetings with some of the respondents.

3.6 VALIDITY OF RESEARCH INSTRUMENT

For face and content validity, the researcher provided enough information so that the internal examiner was able to determine how closely the interview and discussion group questions matched the research situation and whether the findings will be useful. The internal examiner made some changes.

3.7 RELIABILITY OF RESEARCH INSTRUMENT

To confirm its reliability, the questions on the interview guide were asked from some of the researcher's colleagues who are not part of the target population. To reinforce and assess the reliability of the instrument in this research, other staff were asked the same questions to ascertain the need for effective information security strategy to prevent e-fraud in the bank.

3.8 DATA ADMINISTRATION AND COLLECTION

3.8.1 DATA FROM GROUP DISCUSSION

The researcher obtained the required data through the group discussion session. Prior to the session, the researcher took time to explain the purpose of the research to the participants. The researcher also spent time getting their buy-in and cooperation.

Respondents were assured them that their comments would be considered as their professional opinions. They were also assured that they would be allowed sufficient time to make useful contributions to help the business.

The researcher invited the participants verbally, meeting each of them in the office individually. After their acceptance of the invitation, all participants agreed on a venue for the group discussion. The meeting room in the head office was to be used. The researcher liaised with

the corporate services department and made other preparations required to ensure that the meeting would be conducted successfully.

All six invited participants attended the meeting on the agreed date and the discussions were held at the designated venue. The participants were allowed to share their views and discuss opinions or points raised during the meeting. The meeting was originally scheduled to last for four hours, but eventually ran for an extra 12 minutes.

3.8.2 DATA FROM INTERVIEWS

The means of data collection was gathered information from interviews and document review. The researcher used his phone to record the interviews with the interviewees. The researcher had earlier informed the sample size and intended interviewees informally during conversations with them physically via chats and emails. This enabled a better reception during the interviews. A total of nine people were interviewed; though the researcher tried to interview one more person. The researcher also has a rapport with most of the interviewees and this elicited more responses from them as they were comfortable with the researcher. The researcher's role was primarily that of a listener. The researcher also relied upon the interpersonal skills acquired over the years (and especially through courses taken as part of the BSN MBA programme) to know when and how to ask the questions. Each interview was scheduled to hold for about 40 to 45 minutes due to the busy nature of each staff on their respective desks, but some of the interviews lasted for about 50 minutes.

3.9 ANALYSIS OF DATA

The researcher chose to analyse the data obtained from the group discussion and interviews using a qualitative approach because it allowed the researcher to participate in the research setting. The researcher gathered information from interviews and documentary evidences (internal reports from financial control department), analysed the data from these sources, observed and studied certain patterns and was able to draw the researcher's conclusions based on the findings therein. In addition, he was able to present gathered information in a qualitative format. The details of the analyses and a summary of the discussions are presented in chapter four.

3.11 CONCLUSION

This chapter described the research design and methodology in detail. It described the target population and sample size for the survey. It also discussed the methods used in collecting and analysing the researcher's findings.

The next chapter presents the results of the analysis of the data obtained from the discussions and the researcher's findings.

CHAPTER 4

4.0 RESULTS AND FINDINGS

4.1 INTRODUCTION

This chapter presents the data collected through the process outlined in chapter three. It also contains the interpretation of the data as well as supporting information of the findings.

4.2 SAMPLE PROFILE

As earlier discussed in chapter 3, a group discussion and in-depth interview questions were developed. A total number of fifteen (15) members of senior staff made up the sample size. Six management staff were engaged in the group discussion and nine team leads were interviewed. A sample of the In-depth interview questions and group discussion question are presented in the appendix.

4.3 PRESENTATION OF RESULTS

4.3.1 RESEARCH OBJECTIVE 1

The objective is to understand and examine the current information security management strategy in EBL with comparison to best practice. In providing answers to research question one, discussion question 1-6 and interview question 1-3 provide answers to this.

4.3.1.1 DISCUSSION GROUP

Discussion 1: What is the current practice like in the Planning of Information Security in the bank?

Discussant	Response
Discussant 1	IT Group and information security group are responsible for the planning of information security in the bank as against involving the management and the board to ensure their oversight
Discussant 2	I agreed with the CIO. IT and Information security plan the information security for the Bank
Discussant 3	The IT compliance of compliance group ensure that the bank's various policies and standards are being adhered to. My group also benchmark the current practice with the regulatory standards such as CBN

Discussant 4	On a yearly basis, the audit group comes up with the audit program with the scope and objectives of audit. Information Security Audit is also included in the plan to ensure the assurance that the bank's IT assets are protected
Discussant 5	We work with IT group to come up with policies and standards that governs IT activities and how the bank can be protected from IT related risk

Table 4.1: Discussion on Research Question 1

Discussion 2: How is the current Monitoring and Reviewing Process of Information Security like in the bank?

Discussant	**Response**
Discussant 1	The process not clearly defined but the information security group follows up with various gaps identified by internal auditor, external examiners and compiance group to ensure adequate and timely remediation of gaps discovered
Discussant 2	There is no structure monitoring and review process in the bank as far as information security is concerned
Discussant 3	The current monitoring and reviewing processes are runned in Silos, this is part of the information security group processes. These processes need to be reviewed and all stakeholders and managements need to be involved
Discussant 4	There is no proper monitoring and reviewing process is place. Currently, there is no security incidence and event monitoring solution in place. Audits are not enable on all our critical systems talk less of monitoring or reviewing. This makes it difficult to detect or review any security incidence.
Discussant 5	There is no defined Monitoring and Reviewing Process, even the technology and man power to run the process does not exist

Table 4.2: Outcome of Discussion 2

Discussion 3: How is the current Maintenance and improvement of Information Security like in the bank?

Discussant	Response
Discussant 1	The information security group is responsible for the maintenance and improvement of information Security
Discussant 2	The current maintenance and improvement of information security is maturity level 1. The maintenance and improvement of information security is defined in the information security policy but the resources and technology that is required is not available
Discussant 5	The man power for the maintenance and improvement of Information Security in the bank is yet to be fully built and the also lack the required tools to keep this running.

Table 4.3: Outcome of Discussion 3

Discussion 4: What are the available information security related Documents and records in the bank?

Discussant	Response
Discussant 1	The following documents and standards exist: (i) information security policy (ii) IT Policies (iii) IT Procedures
Discussant 2	I am only aware of the information security policy even though not sign off by any members of the senior management
Discussant 3	Information Security Policy
Discussant 4	(i) Information Security Policy (ii) IT audit programme
Discussant 5	These are the available information security related document and records in custody of information security group (i) information security policy (ii) Application Security Standard (iii) Server Hardening Standard (iv) Database Security Standard (v) Anti-Virus Procedure
Discussant 6	I am aware of information security policy

Table 4.4: Outcome of Discussion 4

Discussion 5: How do the management view information security management in the bank?

Discussant	Response
Discussant 1	Information Security is seen as IT business
Discussant 2	Top management sees information security management as IT and information security group responsibility
Discussant 3	As an integral part of IT functions
Discussant 4	Information security is perceived as show stopper to business activities
Discussant 5	Information security is seen as part of IT and the management find it difficult to invest in it as they believe they have already invested heavily in IT
Discussant 6	Information security is perceived as a sub-function of IT

Table 4.5: Outcome of Discussion 5

Discussion 6: Is the Top Management committed to the practice of information security?

Discussant	Response
Discussant 1	Not at all, we are trying to let them be committed to the practice of information security
Discussant 2	No, we are yet to receive their commitment
Discussant 3	As at now, management is yet to be committed to the practice of information security
Discussant 4	Absolutely, No
Discussant 5	Top management commitment is a critical success factor for information security but it is unfortunate that we are yet to get their buy in
Discussant 6	No, because they are yet to be convinced about the needs for information security

Table 4.6: Outcome of Discussion 6

4.3.1.2 INTERVIEW QUESTION

Question 1: How is access control to systems, application and network in EBL handled based on each staff job's functions?

Interviewee	Response
Respondent 1	Access control to systems, application and network is not adequate. Some staff of Information Technology hasve excessive access to systems
Respondent 2	Privilege account are not managed properly as some IT staff have access to this account. Some of the accounts are used to carry out routine IT admin functions
Respondent 3	Some members of staff access control are in line with their jobs' function while some members of staff access to systems are not in conformity with their job's function.
Respondent 4	Least Privilege Principle is not defined for some IT staff as some programmers have access to production environment.
Respondent 5	There is no defined policy for access control in the bank.
Respondent 6	Access to systems application and database are based on job's functions but some staff of network administration access are not properly defined
Respondent 7	Access to the bank's systems, application and network in EBL is in conformity with the bank information security policy
Respondent 8	The bank's access control to IT infrastructure is not full proof. There is always room for improvement
Respondent 9	All access to systems are handled properly but there are some exceptions to this based on the job's demand.

Table 4.7: Outcome of Interview Question 1

Question 2: What is the management perception of Information Security Management?

Interviewee	Response
Respondent 1	Management does not see the reasons for reviewing the activities of information management

Respondent 2	Executives management do not put in place control to ensure good practice for information management
Respondent 3	Management disposition to information security is indifferent
Respondent 4	Management is not driving information security management
Respondent 5	There is no management buy in to information security management. They need to drive it to ensure its effectiveness
Respondent 6	There is no financial support from management for the management of information security as they feel that there is no financial benefit
Respondent 7	Management sees information security management as part of IT and believe lots of money has already been allocated to IT and there is no need to spend more on information security
Respondent 8	Management disposition to information security is changing as there is now provision for it in the budget.
Respondent 9	Management has negative disposition to information security as they believe that their main responsility is to ensure profitability not knowing the security posture can as well impact on the profitability of the bank

Table 4.8: Outcome of Interview Question 2

Question 3: How is the information security perceived by staff of EBL?

Interviewee	**Response**
Respondent 1	Staff sees information security as a show stopper for them in delivering their daya to day work.
Respondent 2	Staff sees information security activities such as password complexities, segregation of duties among other as waste of time.
Respondent 3	Staff are not comfortable with compliance when it comes to adhering to the bank's information security policy
Respondent 4	Some staff sees it as a must to have especially staff in information technology group and some do not understand what it entails

Respondent 5	Staff has negative culture towards information security as they has little level of awareness towards the subject matter.
Respondent 6	The awareness level of staff whose jobs are related to information systems or technology is ok while non-technical staff seems to be nonchalant about information security
Respondent 7	IT staff sees it as a means to protect the bank IT assets from attackers while the general staff seems not to understand it
Respondent 8	Quite number of staff has little knowledge about information security while the technical staff especially the IT staff sees it as very necessary
Respondent 9	Staff sees it as a means to ensure that customers' data are protected even though they are not ready to practice it because they see it as a burden

Table 4.9: Outcome of Interview Question 3

4.3.2 RESEARCH OBJECTIVE 2

The objective is to establish information security gaps in EBL. In providing answers to research question two, discussion question 7 and interview question 4-12 provide answers to this.

4.3.2.1 DISCUSSION GROUP

Discussion 7: What are the gaps in the planning of Information Security in the bank?

Discussant	**Response**
Discussant 1	Lack of management involvement in the planning of information security in the bank
Discussant 2	Lack of management support in the planning of information security in the bank
Discussant 3	The planning of information security is supposed to be driven by top management and the executives to ensure that information security align with the business objectives. Currently, information security objectives do not align with business objectives
Discussant 4	The planning of information security is carried out without taking the stakeholders along

Discussant 5	The planning of Information Security in the bank is managed by information security group. For ISMS to be effective top management leadership is required to easily integrate information security into business

Table 4.10: Outcome of Discussion 7

4.3.2.2 INTERVIEW QUESTIONS

Question 4: Is there standard procedures or approvals before an IT change is made that will impact the bank information system?

Interviewee	**Response**
Respondent 1	The IT change management process is run in Silos by IT department, all stakeholders are not involved in the process and senior management approval is not required.
Respondent 2	There is an IT Change management procedures and approval is not required for change that will impact on the bank information system.
Respondent 3	The IT change management procedure is inadequate and there is no provision for management approval before a change is deployed to production
Respondent 4	There is a standard procedures for IT change but not sure whether it adequate
Respondent 5	The current IT procedures do not address change that has major impact on the bank's information systems as critical stakeholders are not carried along in the process, management is not also aware of IT changes
Respondent 6	Yes, there is standard procedures for IT changes, also Head, IT operations sign off all changes before implementation
Respondent 7	There is standard procedures for IT changes and IT senior staff approves all changes that will impact the bank information system before go live
Respondent 8	There is change management process even though the process is yet to be mature, we are working on how to improve the process to ensure that all stakeholders are carried along and get senior management or representative approval before deployment

Respondent 9	There is a standard procedures for IT changes and supervisor and head of IT operations approvals are gotten before implementation

Table 4.11: Outcome of Interview Question 4

Question 5: Is the network, host, and application(s) vulnerable to attacks from the internet or intranet which result in financial/reputational loss?

Interviewee	**Response**
Respondent 1	Yes, there are few cases of incidence of financial loss due to lack of adequate control from the network and application layers.
Respondent 2	The bank's network is vulnerable to attacks, the bank losses huge amount of money due to the attack in the last one year
Respondent 3	The bank has suffered from reputational damage due to financial loss cause by the bank's vulnerable network and application.
Respondent 4	Electronic fraud ranked first based on the bank's fraud statistic and this was as a result of inadequate countermeasure in the bank network, systems and application.
Respondent 5	The lack of adequate control to mitigate risk of financial loss and reputational damage has exposed the bank immensely
Respondent 6	The bank's network, systems and application are protected to a reasonable extent. However, 100% protection cannot be guaranteed as there are new vulnerabilities every day in cyber word. The bad guys exploit on this and take advantage of the systems for their financial gains.
Respondent 7	There is no full proof controls against attacks from malicious people. Even though there is a measure of controls against attacks, the bank still suffer attacks from hackers some of these resulted in financial loss and image damage to the bank.
Respondent 8	IT department try as much as they can to protect attacks by making sure that adequate controls within the provided resources are implemented. However, these controls are not enough as the management need to invest more on information security to mitigate the risk of financial losses due to hacking of the bank's systems

Respondent 9	Some applications and operating systems are vulnerable to attack from the internet and even the bank's intranet.

Table 4.12: Outcome of Interview Question 5

Question 6: Can malicious user easily access, modify, or destroy data or services within the system due to the current information security practices?

Interviewee	**Response**
Respondent 1	Yes, malicous user can easily carry out unauthorised access or modification on the bank network due to the present configuration.
Respondent 2	Malicious users can gain access to the bank systems to carry out fictitious activities due the insufficient security practices in the bank
Respondent 3	It is possible for a malicious user to gain access to carry out un-approved activities because of the current information security practices. The bank is not complying to all the documented standards and policies
Respondent 4	Yes, malicious user can access, modify or destroy data or services within the system as revealed by the bank's fraud statistic. There are more incidences of computer related fraud
Respondent 5	There likelihood for a malicious user to gain access, modify and destroy data or services is high because the current information practices in the bank is not good enough.
Respondent 6	It is possible for a malicious user easily access, modify, or destroy data or services within the system as it is impossible to achieve 100% protection in information security
Respondent 7	Yes, depending on the skill set of a malicious users
Respondent 8	Based on lack of management commitment to information security and the bank lacks intrusion and prevention system (IPS) that will detect/prevent any intrusion to the bank's systems. Management is yet to approve the purchase of this tool
Respondent 9	Yes it is possible.

Table 4.13: Outcome of Interview Question 6

Question 7: Is there adequate technical control in place to protect the bank's network to prevent financial loss?

Interviewee	Response
Respondent 1	No, the technical control in place is not sufficient.
Respondent 2	No, as it is very obvious
Respondent 3	The technical control in place is not adequate
Respondent 4	Just like I mentioned earlier if we have adequate technical control in place to prevent financial loss, computer related fraud will not rank first in the bank's fraud statistic
Respondent 5	If the technical control is adequate, the bank would not have been so exposed to financial losses in our electronic platforms
Respondent 6	No, there is no technical control that is adequate that is the reason for defence in depth approach to information security
Respondent 7	Yes, but the bank still need to invest more on various technical tools to prevent financial loss
Respondent 8	Investment need in information security is required for the bank to have full assurance in the technical control in place. Hence, the bank lack tools to adequately protect the bank's network against financial loss
Respondent 9	Not adequate, there are lots of technological control not in place as these requires money for the acquisition

Table 4.14: Outcome of Interview Question 7

Question 8: Is Security Review and assurance part of business process and IT operational activities?

Interviewee	Response
Respondent 1	Yes, it is as the internal audit group carry out the review of IT activities on a periodic basis(every quarter). This audit programs are being reviewed on a yearly basis

Respondent 2	Yes, routine security review of IT operations is part of key performance indicators (KPIs) for all staff of IT control
Respondent 3	Yes, security review and assurance is part of business process and IT operational activities of the bank as my unit conduct compliance assessment from time to time to ensure that we are doing the right thing.
Respondent 4	I do not believe that we practice what we say because if the required units are doing their job as required they would have let the management know our lapses of IT operations activities in order to make informed decision.
Respondent 5	Yes, there is from various compliance units such as IT Control, IT audit, IT risk and IT security. The question should be if there is management review and oversight of the various reviews conducted?
Respondent 6	Yes, as my unit is doing its part and the reports are sent to IT management
Respondent 7	Yes, Security Review and assurance is part of business process and IT operational activities
Respondent 8	Yes there is but there is no active action plans to remediate all the security lapses identified. Though, IT is doing its part but management support will be required to remediate the major issues.
Respondent 9	Yes security review and assurance is part of business process and IT operational activities though the manner at which this is conducted may not be adequate.

Table 4.15: Outcome of Interview Question 8

Question 9: Is there a strategy for Enforcement of Information Security in EBL?

Interviewee	**Response**
Respondent 1	No such strategy exist
Respondent 2	I am not aware of such
Respondent 3	Yes, partly IT compliance ensure enforcement of the agreed information security policies and procedures
Respondent 4	Not at all

Respondent 5	There is no clearly defined strategy for enforcement of information security in the bank
Respondent 6	I am not sure if such strategy exist
Respondent 7	No, there is no strategy for Enforcement of Information Security in EBL
Respondent 8	No. Such strategy needs to be driven by senior management.
Respondent 9	No. It doesn't exist

Table 4.16: Outcome of Interview Question 9

Question 10: Is there frameworks that cover all aspect of Information Security Management.in EBL?

Interviewee	**Response**
Respondent 1	No, the current information security policy is not comprehensive
Respondent 2	Even though we have various security policies and standards they do not cover all aspect of information security management
Respondent 3	Yes, partly IT compliance ensure enforcement of the agreed information security policies and procedures
Respondent 4	Partly yes and partly no because what is currently on ground does not cover all aspect of Information Security Management.in EBL
Respondent 5	The bank's information security policy is not robut enough, there is need for proper review to ensure that all aspect of information security management is covered and in line with business objectives
Respondent 6	Yes, there is frameworks that cover some aspect of Information Security Management.in EBL. This need to be reviewed to ensure it completeness
Respondent 7	No, the current framework does not cover all aspect of Information Security Management.in EBL

Respondent 8	The current framework need to be reviewed to ensure it covers all aspect of Information Security Management.in EBL
Respondent 9	No, the current framework need to be revamped

Table 4.17: Outcome of Interview Question 10

Question 11 EBL culture, ethics and behaviours reflect a secure IT environment?

Interviewee	**Response**
Respondent 1	No, there is need for cultural change to information security
Respondent 2	EBL organisational structure does not reflect a secure IT environment
Respondent 3	Members of staff are still struggling security culture in the organisation
Respondent 4	No, the manner at which staff and management carry out IT activities does not reflect a secure IT environment
Respondent 5	No, EBL culture, ethics and behaviours reflect a secure IT environment
Respondent 6	The bank has poor information security culture, ethics and behaviours
Respondent 7	Most staff especially those whose job roles do not relate with information security has bad security culture
Respondent 8	No, as there is no driver to information security culture, ethics and behaviours. It is easy for staff to develop the culture if it is embedded into organisational culture by the management
Respondent 9	To some extent, the EBL culture, ethics and behaviours do not reflect a secure IT environment

Table 4.18: Outcome of Interview Question 11

Question 12: Are you adequately trained on Information Security Management principle as it relates to protection of bank's information asset?

Interviewee	**Response**

Respondent 1	I have not gone for any training on information security management trainig for the past three years
Respondent 2	Not at all
Respondent 3	Since the time I became the Head, IT Compliance, the bank is yet to send me to any formal training on Information Security Management principle
Respondent 4	No, I am yet to go for any technical training on IT forensic as it relates to my job functions
Respondent 5	No, there is no training plan for such and I have not gone for any bank's sponsored training except for the one I enrolled
Respondent 6	No, I have always been training myself as the bank makes no provision for such training
Respondent 7	No, I am not adequately trained on Information Security Management principle as it relates to protection of bank's information asset
Respondent 8	IT is working with the management to ensure that all technical training on Information Security Management are being planned for with the management to ensure that bank's information assets are well protected
Respondent 9	No, I have not gone for any bank's sponsored training on Systems and Unix security

Table 4.19: Outcome of Interview Question 12

4.3.3 RESEARCH OBJECTIVE 3

The objective is to establish consequence of information security gaps on the bank and its asset. In providing answers to research question two, discussion question 8-10 and interview question 13-16 provide answers to this.

4.3.3.1 DISCUSSION GROUP

Discussion 8: Has the bank's network, application and systems been infiltrated with Virus or Malware?

Discussant	**Response**

Discussant 1	Virus and Malware are continous threats faced by the bank.
Discussant 2	Yes, we have recurring infiltration of virus and malware on our network, application and systems
Discussant 3	Yes, almost everyday
Discussant 4	Yes, this is a growing concerns
Discussant 5	Though most of our critical servers are not directly facing the internet, however the workstations are vulnerable as we receive daily alert of virus and malware via the workstation. Though the risk infiltration is low as no users of workstation has admin right which is the type of right required by most malware to carry out malicious activities.
Discussant 6	There are several cases of infiltration especially for staff handling sensitive data

Table 4.19: Outcome of Discussion 8

Discussion 9: Has the bank been exposed to Hacking that lead to financial in the past two year?

Discussant	**Response**
Discussant 1	It is unfortunate that the bank is exposed to hacking which has resulted in great financial loss to the bank.
Discussant 2	Yes
Discussant 3	Yes
Discussant 4	Yes
Discussant 5	Yes
Discussant 6	Yes

Table 4.20: Outcome of Discussion 9

Discussion 10: What are the customer's (internal or external) complaints like on the unauthorized access or modification on their accounts?

Discussant	Response
Discussant 1	We always have different complaints ranges from password compromise to unauthorise transactions from our external customers. We seldom have complain from internal customes on this except for the major breach that happens in which on of the administrators account were compromised to carry out unauthorised activities which resulted in great financial loss to the bank.
Discussant 2	We receive dozens of report from the customers service department on unauthorised access or modification on customers' accounts
Discussant 5	The complaints from customers ranging from phishing attack, social engineering, password compromise
Discussant 6	We had several complaints from customers on most of our e-payment platforms that their passwords were compromised and unauthorised transactions were carried out on their accounts.

Table 4.21: Outcome of Discussion 10

4.3.3.2 INTERVIEW QUESTIONS

Question 13: What is the rate of major breaches involving sensitive or confidential information for the past one year?

Interviewee	Response
Respondent 1	The rate at which breaches such as phishing, social engineering and identity theft occur have been on the increase for the past one year
Respondent 2	There are more incidences of electronic fraud for the past one year.
Respondent 3	There has been several complaints from the customers that some transactions occur on their electronic platforms which they do not initiate. Some complaints that their account details were revealed to an outsider and they were wondering how it happened
Respondent 4	The fraud on the electronic platform such as mobile banking, online banking has been on the increase as revealed by the bank's fraud statistic. I will be willing to share the statistic with you. Based on the statistic alone,

	88% of the fraud are as a result of ineffective information security strategy. Refer to appendix IV for details.
Respondent 5	Based on our yearly risk loss index, the rate of major breaches involving sensitive or confidential information for the past one year has increased by 30% which is very alarming
Respondent 6	We have more incidents reported this year as a result of breaches involving sensitive or confidential information.
Respondent 7	There are more complaints from the customers' end that their accounts details such as password, balance have been compromised
Respondent 8	Based on the yearly report of IT, there is 28% increase in reported incidence as a result of breaches involving sensitive or confidential information last year ending (2015) compare to 2014.
Respondent 9	The rate of breaches involving sensitive or confidential information has been on the increase for the past one year

Table 4.22: Outcome of Interview Question 13

Question 14: What is the rate of stealing customers' data at rest or in motion for the past 3 months?

Interviewee	**Response**
Respondent 1	In the last three months we investigated about 30 cases of customers whose PIN, password and other cardholder data information were compromised.
Respondent 2	Quite numbers of compromised cases were recorded in the last three months
Respondent 3	There are about five legal cases due to stolen customers' data either at rest or in motion
Respondent 4	IT audit and my unit always collaborate to investigate cases of stolen data, based on the report there are about 30 cases

Respondent 5	Based on report collated from various risk champions, there are more cases of such incidence in the last three months
Respondent 6	The rate of occurrence of incidence due to stolen data has been increasing in the past three months.
Respondent 7	I may not be able to say the exact rate but I know that we have more incidence of customers' stolen data in the past three months
Respondent 8	There are more incidences of such in this quarter than the previous quarter.
Respondent 9	There are lots of reported cases for the past three months

Table 4.23: Outcome of Interview Question 14

Question 15: What is the rate of malware and virus infection of sensitive data for the past one month?

Interviewee	**Response**
Respondent 1	It is evident that there is presence of malware and virus infection on the network but cannot really determine the effect on sensitive data in the last one month.
Respondent 2	About eight of the systems of staff especially the IS control systems that have some sensitive data were corrupted with malware and virus, those systems were formatted before restoring the data back.
Respondent 3	About 30% of the banks' workstations were infected at one point or the other, among the workstations some of them have sensitive data
Respondent 4	Some of the banks' workstation have sensitive data and large numbers of the banks' workstation have been infected with malware
Respondent 5	More than 25% of the systems in our networked were infected with malware. Some of the systems have sensitive data on it.
Respondent 6	We monitor the spread of malware and virus on a daily basis and take active measure to ensure that all systems in our network have antivirus

	install, up to date. We centrally push antivirus, scan any infected systems and push update. Last month ending about 29% of the systems on our network were infected due to outdated antivirus as at that particular day. However, we were able to carry out fixes on those systems in last than three days.
Respondent 7	There has been increase in the rate of malware/virus infections on our network but we were able clean the network of virus infections
Respondent 8	The occurrence of malware and virus have been on the increase for the past one month but we have a robust antivirus program to manage this as we were able to contain this
Respondent 9	There has always been malware and virus threat through our windows platforms and the last one month is not an exception but the good news is that we were able to monitor and manage this.

Table 4.24: Outcome of Interview Question 15

Question 16: Has the bank suffered financial loss and reputational damage due to inefficient information security strategy?

Interviewee	**Response**
Respondent 1	The bank has suffered greatly as a result of ineffective information security strategy
Respondent 2	Yes, the bank has suffered from both financial loss and reputational damage as a result of ineffective strategy to prevent this
Respondent 3	It is unfortunate that the bank image has been dragged in the mud due to compliance with the CBN roadmap on IT security. The bank has lost several millions of naira as a result of this.
Respondent 4	Yes, the bank has always been losing financial as a result of inefficient information security strategy. This is not good for our reputation as a bank.
Respondent 5	Lately, the bank has been exposed to financial and reputational risk due inefficient information security strategy

Respondent 6	The bank has lost some money due to inefficient information security strategy
Respondent 7	There has been escalating e-fraud which leads to financial and reputational loss as a result of inefficient information security strategy
Respondent 8	Yes, the bank profitability has been greatly impaired as the bank has lost huge amount of money as a result of lack of management commitment to information security.
Respondent 9	Yes of course, this need to be addressed immediately else the bank might lose the market to competitors.

Table 4.25: Outcome of Interview Question 16

4.3.4 RESEARCH OBJECTIVE 4

The objective is recommend effective ways by which bank's e-fraud can be prevented as informed by best practice. In providing answers to research question two, discussion question 11-12 and interview question 17-18 provide answers to this.

4.3.4.1 DISCUSSION GROUP

Discussion 11: What can be done to improve the existing information security strategy?

Discussant	**Response**
Discussant 1	The information security objectives need to be derived from the business objectives to ensure alignment.
Discussant 2	Senior management oversight is required to revamp the existing strategy. Need for gap assessment of the existing information security strategy compare with the industry standard and then the bank need to develop a strategy to close the identified gaps
Discussant 3	Aligning of existing strategy with industry standard such as COBIT 5, NIST, PCI DSS or ISO 27001 because such standards are proven and tested over period of time to be effective

Discussant 4	Continuous independent review of information security strategy with all the stated controls and audit reports of findings should be sent to senior management.
Discussant 5	Network revamp to ensure secure network, follow a secure practice for the bank's application and systems, implementation of file integrity monitoring to detect any unauthorised change, implementation of SIEMs to proactively monitor users activity and act before security events crystalize to fraud.
Discussant 6	Bank-wide information security awareness, creating a roadmap for the desired state and get management buying in order to improve our existing strategy

Table 4.26: Outcome of Discussion 11

Discussion 12: What are the controls to be implemented to prevent e-fraud?

Discussant	**Response**
Discussant 1	In order to prevent e-fraud in the bank a combination of administrative, technical and physical control would be required
Discussant 2	To prevent e-fraud in the bank, there should be a robust IT risk management in place and top – bottom approach need to be considered to be effective
Discussant 3	Complying the regulatory standards on the requirements for electronic systems such implementation of two factor authentication, maker-checker for all transfer, keeping of audit trail will serve as deterrent practice to prevent e-fraud
Discussant 4	Implementation of fraud monitoring systems to monitor transactions on all our electronic platforms, flag any suspicious pattern in order and stop any discovered fraudulent activities.
Discussant 5	Implementation on Intrusion Prevention Systems. This system can proactively detect any malicious packet or hacking attempts on the bank's

	network, systems or applications. This solution can be integrated with SIEM as earlier discussed for optimised utilisation

Table 4.27: Outcome of Discussion 12

4.3.4.2 INTERVIEW QUESTIONS

Question 17: What can be done to ensure that managements are accountable for Information Security Management Strategy?

Interviewee	Response
Respondent 1	Managements need to be made aware of all the security assessment conducted by internal audit group, not just having the report but drive the action plans for remediation.
Respondent 2	Managements need to ensure that information security is an integral part of the business not just seeing it in silos
Respondent 3	Compliance to information security standards need to be part of job's functions of the management. Management drive is required to ensure compliance to the bank information security strategy
Respondent 4	Management oversight of all information security activities will make management to be accountable for security strategy
Respondent 5	To ensure that managements are accountable for information security management strategy, there will be a need for gap assessment to determine our current state, analyse and plan how to get to the desired state and come up with traction. Throughout this phase, management need to be engaged, this can be achieved by instituting information security steering committee comprising different management stakeholders.
Respondent 6	Managements should be made responsible for any security breaches as a result of their lack of support.
Respondent 7	Effective information security management strategy need to be driven from the top, management need to be aware of the various information security initiatives before they can be accountable for it.

Respondent 8	Boards and senior management need an awareness for them to be able to understand their role/accountability in information security management. This can better be achieved by engaging a consultant on formal boards and senior managements' education on information security.
Respondent 9	In order to ensure that management are accountable for Information Security Management Strategy, they will need to understand the implication of lack of good strategy and how it can affect the business. I believe information security awareness is very critical to achieve this.

Table 4.28: Outcome of Interview Question 17

Question 18: What measures can be put in place to prevent the recurring e-fraud in the bank?

Interviewee	**Response**
Respondent 1	In order to prevent e-fraud in the bank, defence in depth mechanism which is a layer security need to be put in place. We will to combine different controls both technical and administratie at different layes such as network, systems and application to achieve this.
Respondent 2	From my point of view, the bank need to ensure that all our public facing application/systems such as email and online banking are well protected by following industry standard on information security. Some of the practices to be adopted are: good authentication and authorisation practice; placing all public facing application behind a firewall and implementation of intrusion prevention system.
Respondent 3	The bank need to ensure strict compliance with information security best practice such as ISO 27001 and COBIT 5 to prevent the recurring e-fraud in the bank
Respondent 4	To prevent the recurring e-fraud in the bank, there will be needs: for investment in solution that can monitor and detect e-fraud before it happens; to improve on the bank's information security practice and for information security awareness campaign for staff and customers
Respondent 5	As I mentioned earlier, there will be a need for gap assessment to be based on industry standard such as PCI DSS, ISO 27001 and COBIT 5,

	the bank need to come up with a strategy of the bank's desired maturity level and set out action plans in achieving the sets objectives.
Respondent 6	The bank need to invest in IT security by ensuring that various tools to ensure that the technical controls are achieved are in place.
Respondent 7	To prevent the recurring e-fraud in the bank, the bank needs to tighten up the information security practice by ensuring that it aligns with IT security best practices, there will be need for adequate technical controls such as segmentation of the bank network, implementation of intrusion prevention systems (IPS) and Security Incidence and Event Monitoring (SIEM).
Respondent 8	To prevent the recurring e-fraud in the bank, we will need to look at this from people, process and technology. First and foremost people need to do what they are supposed to do to ensure adequate protection of the bank's IT asset, our customers, staff and management need to be informed that information security is everybody responsibilities. Our processes need to be revamped to ensure a secure environment and the bank need to invest on security tools.
Respondent 9	Implementation of various controls across our network, systems and application. Some of this control can be implementation of 2 factor authentication and implementation of SIEM

Table 4.29: Outcome of Interview Question 18

4.4 SUMMARY OF FINDINGS

From the research question 1 (How information security management is practiced in EBL?) the findings are as below:

1. Management is not involve in the planning of information security management. The planning is carried out in silos without carrying all the stakeholders along
2. There is no management buy in the current information security strategy
3. The current monitoring/reviewing and maintenance process of information security management is ineffective as the bank lack the resources such as man power and technical tools to make this functional
4. Access control to application, network and systems is not adequate

5. Poor awareness by members of staff and management to information security

From the research question 2 (What are the gaps of information security management strategy in EBL?) the findings are as below:

1. Information security objectives do not align with business objectives because of lack of management buy and support
2. Inefficient IT change management process as stakeholders and managements are not included in the process
3. The bank's network, systems and application are vulnerable to attacks from malicious people
4. The technical control in place to protect the bank's against attack or electronic fraud is insufficient
5. The current policies and standards that governs the management of information security in the bank is not sufficient as its enforcement is not clearly defined in the documents
6. IT security personnel are not adequately trained on the management of information security and members of staff are not aware of the need for information security

From the research question 3 (What are the consequences of these gaps on the bank and its information asset?) the findings are as below:

1. Ineffective information security strategy has exposed the bank to malware and virus attack
2. The bank has suffered greatly from financial loss as a result of hacking through the attack vector such malware, social engineering and malicious user through our electronic platform
3. Customers confidence in the bank has been eroded due to e-fraud on their accounts which results in reputational damage/financial losses for the bank
4. E-fraud is prevalent in Enterprise bank and has resulted in huge financial loss to the bank due to ineffective information security strategy

From the research question 4 (How can the bank prevent e-fraud?) the findings are as below:

1. Management commitment and buy in is required in the bank's information security strategy to ensure its alignment with business objectives
2. Implementation of robust risk management process is required
3. Benchmarking the existing practice with best practice to identify the gaps and comes up with strategy to close those gaps will be required
4. Implementation of technical controls for the prevention of e-fraud such as SIEM, IPS, fraud management systems

4.5 DEDUCTION OF FINDINGS

The researcher's findings corroborates the notion in the literature review on the need for information security management in order to mitigate risk against confidentiality, integrity and availability of information assets in the bank as informed by Usman and Shah (2013), Harris (2013), Whitman and Mattord (2012), COBIT (2012), NIST (2014), Klie (2015) and ISO 27001 (2013) as explained in section 2.2. Effective strategy need to be developed in EBL as being focused on the strategy session. Steps and how to develop information security management strategy as informed by Ricky and Monique (2014), LeVque (2006), Young and Windsor (2010), Pironti (2010) and Whitman (2003) as explained in 2.3.

EBL need to build effective information security strategy with the objectives of balancing the need to secure information assets against the need to enable business, ensuring compliance and maintaining cultural fit as informed by Kayworth and Whitten (2012), Evans (2015), Istikoma *et al* (2015), Chen *et al* (2012), Thompon *et al* (2006), Da Veiga and Eloff (2010), Alhogail and Mirza (2014). There is also need to carry out intensive gap assessment in order to determine the current state of data security strategies and the desired state in order to improve on the security posture. This is necessary to know whether the bank derives the benefit of effective information security strategy or faces the consequences of ineffective information security strategy as informed by Evans (2015) and PTAC (2011).

To prevent the recurring e-fraud in the bank as established in the findings strategy to prevent this need to be established as informed by Behdad et al (2012), ACI (2012), NEFF (2014) and Cappelli et al (2012). Furthermore, management decision is also very key in combating e-fraud as analysed in the findings various frameworks also explained how to combat e-fraud by effective information security strategy as informed by NIST (2014), Shen (2014), Lei (2014); ISACA (2012), De Haes (2013), Zhang and Le (2013), PCI (2015) and Klie (2015).

4.6 CONCLUSION

This chapter presented the analysis of the findings from the surveys used in this research (i.e. group discussion conducted with management staff and interviews team leads of staff whose jobs' functions are related to the management of information security). It also provided a

descriptive summary of the data collected. The next chapter gives the researcher's recommendation and options from results analysed.

CHAPTER FIVE

5.0 GENERATING AND EVALUATING SOLUTION ALTERNATIVES

5.1 INTRODUCTION

This chapter provided an analysis of the findings gathered through the research, as well as the interpretations of the findings. This chapter draws conclusions from the study. It also presents recommendations as well as various implementable options.

5.2 RECOMMENDATION

Based on the deductions from the findings in 4.4, it can be observed that the bank's information security strategy is ineffective which result in recurring e-fraud in the bank. There is need to carry out intensive gap assessment in order to determine the current state of information security strategy and the desired state in order to improve on the security posture of the bank. The analysis of the data gathered in the research revealed the ineffectiveness of the current strategy which needs to be improved in order to protect the bank's information asset. Sequel to field analysis, literature review, and the researcher identified 3 set of options to adequately protect the banks against e-fraud. The benefit of each option was evaluated and the cost of implementation was described. The options are as follows:

1. Adopting PCI DSS 5 Framework
2. Adopting COBIT 5 for Information Security Framework
3. Adopting NIST Cybersecurity Framework

5.2.1 ADOPTING PCI DSS 5 FRAMEWORK

According to PCI (2015), PCI DSS Framework is a sets of standards and guidelines to card fraud this is formulated to assist all industries or entities that deal with payment cards. Calder and Williams (2014) also explains that the framework applies to anywhere cardholder information resides as explained in section 2.8.3

Benefits

1. PCI DSS explains in details how to implement all each of the controls
2. The process is very robust to protect cardholder, it also controls and monitors access to cardholder data
3. The standard allows self-appraisal for merchants that processes card data which can form the basis of bias of the assessment report

Disadvantages

1. The scope is limited to cardholder data only

Cost of Implication

1. Cost of Engaging a Qualified Security Assessor for compliance check. This is a recurring yearly cost
2. Cost of Engaging a Consultant to kick start the project

5.2.2 Adopting COBIT 5 for Information Security Framework

ISACA (2012) publication on COBIT 5 frameworks for Information Security is a risk based program methodology which provides comprehensive ways of ensuring reasonable and appropriate security controls for information resources as explained in section 2.8.2 above

Benefits

The benefits of COBIT 5 for information security are (i) to reduce complexity and increased cost-effectiveness as a result of improved and easier integration of information security standards; (ii) to increase user satisfaction with IT security arrangements and outcomes; (iii) to improve integration of IT security controls in the enterprise; (iv) to enhance informed risk decisions and risk awareness; (v) to improved prevention, detection and recovery in a case of fraud; (vi) to reduce impact of security incidents such as hacking and e-fraud; (vii) to enhance support for innovation and competitiveness (viii) to improve management of costs related to the information security function and (ix) for better understanding of information security

Disadvantages

The following are the disadvantages for COBIT 5: COBIT is difficult to implement as it requires great effort to learn and understand the framework because of the large numbers of IT processes and control objectives. The COBIT guidelines do not provide specific details of utilization. According to De Haes et al (2013), COBIT 5 is a complex set of standard.

Cost of Implication

1. Cost of Engaging a Consultant to kick start the project

5.2.3 ADOPTING NIST CYBERSECURITY FRAMEWORK

According to NIST (2014), it is imperative for organizations to describe their current cybersecurity posture; describe their target state for cybersecurity; identify and prioritize opportunities for improvement within the context of a continuous and repeatable process; assess progress toward the target state and communicate among internal and external

stakeholders about cybersecurity risk. This goes a long way in protection of valuable data as well as preventing e-fraud as explained in 2.8.1 above.

Benefits

1. Organisation can use the framework to determine their existing cybersecurity posture whether it is adequate or not, if not develop one from scratch
2. The framework help in setting objectives for cybersecurity that are in agreement with business objectives to prioritize opportunities for improvement/establish a plan for improving or maintaining their cybersecurity
3. The framework is very important to help the management understand their company's security practices thereby enable them see how their company's cybersecurity practices align with the framework's standards, understand where the company's vulnerabilities, and determine if they are doing enough.
4. The framework provides the standardization approach to addressing the approach to cybersecurity concerns
5. It helps the organisation to collaborate by sharing cybersecurity best practices and lessons learned
6. Organisation using the framework will be able to demonstrate due care in cybersecurity incidence by providing the stakeholders with information on the posture.
7. The framework enables the security auditors to be able to evaluate the organisation security posture in one standard format which eliminates the needs for various security compliance document
8. It provides an opportunity for the organisation to better understand the risk imposed by their supply chains which enable the organisation to spend security budgets wisely

Disadvantages

The framework has no enforcement authority; the organisation can use their discretion whether or not comply with the framework. The framework does not clearly define how to protect critical infrastructure it only references various standards. Implementing the framework is not straightforward

Cost of Implementation

Cost of Engaging a Consultant to kick start the project

5.3 DECISION MATRIX

The researcher decided to make use of decision matrix method to make a choice from the options, in order to arrive at objective and better options. The process is tabulated below:

Factors	Cost	Benefit	Timeline	Total
Options				
1	5	4	2	
2	4	4	3	
3	4	5	4	

Table 5.1: Un-Weighted Assessment Of Each Option

Factors	Cost	Benefit	Timeline	Total
Weight	3	5	4	
1	15	20	8	**43**
2	12	20	12	**44**
3	12	25	16	**53**

Table 5.2: Weighted Assessment Of Each Option

Scoring option: 0(poor)- 5 (very good) (Weight allocation 1-5 according to importance)

5.4 SELECTION OF OPTION

From the tables above, option 3 has the highest factor i.e. option 3 is the recommended option, adopting NIST Cybersecurity Framework. This framework is very robust and integrates others framework such as PCI DSS, ISO 27001, COBIT 5 and provides a holistic view of effectively protecting the bank's critical assets to prevent e-fraud.

5.5 CONCLUSION

This chapter focused on the conclusions of the analysis, recommendations and Options that are available to implement effective information security strategy in order to prevent e-fraud in the bank.

The next chapter considers the implementation of the selected option.

CHAPTER SIX

6.0 IMPLEMENTATION

6.1 INTRODUCTION

The previous chapter presented the conclusion, recommendation and options this chapter focuses on the road map to the implementation of the researcher's preferred option to establish effective information security strategy to prevent efraud in the bank, the cost benefit analysis of the preferred option and challenges during the course of implementation.

6.2 IMPLEMENTATION PLAN

The table below illustrates the implementation of the suggested process to protect the bank's and customers' data in EBL:

S/No.	Major Task	Responsibility	Critical Success Factor	Timing
1.	Schedule a meeting with the stakeholders consisting of ED Service Bank, ED Risk, Chief Information Officer, Chief Risk Officer, Chief Compliance Officer, Chief Internal Auditor, and Chief Information Security Officer for briefing on the implementation.	Researcher	Clear and timing communication by the researcher	02/04/2016-16/04/2016
2.	Make the first presentation to the stakeholders.	Researcher	Clear and timing communication by the researcher	17/04/2016-18/04/2016
3.	Submit research findings to executive management and seek a date for presentation.	Chief Information Security Officer	Convincing summary of the findings by the Chief Control Officer	20/04/2016
4.	Make second presentation to executive management and other stakeholders.	Chief Information Security Officer	Clear and timing communication by the Chief Control Officer	23/04/2016

5.	Seek management's approval for the implementation of the preferred option.	Chief Information Security Officer	Chief Information Security Officer Conviction and ability to let management buy into the idea	23/04/2016-30/04/2016
6.	Submit a copy of the approval to all stakeholders for subsequent implementation.	Chief Information Security Officer	Management Approval and sign off	01/05/2016
7	Adoption and Final Implementation	All Stakeholders	Adequate funding by the management	02/05/2016 -18/05/2016

Table 6.1: Implementation Plan

ACTIVITIES	**ESTIMATED COST (₦)**	**NUMBER OF PARTICIPANTS**	**TOTAL COST(₦)**	
External Consultant	20,000,000		20,000,000.00	
Journals, articles and materials	2,000 per participant	100	200,000.00	
Refreshment	1,500 per participant	100	150,000.00	**₦24,850,000.00**
Training Cost/certification for the major stakeholders	150,000 for each participant	30	4,500,000.00	

Table 6.2: Implementation Budget Table

The training/certification of stakeholders would be organized in two batches as all stakeholders cannot attend the training at once, in order not to shut down the business for the period they are away. An introductory meeting which will be held inform of a conference to educate all stakeholders before the commencement of the program. This meeting will be held a week before the first session starts. Mail will be sent as scheduled in the program to the next group to avail them of the training.

Cost Benefit Analysis

The preferred option involved cost of the training, cost of engaging consultant and workshop to all the stakeholders but the benefit of e-fraud prevention as a result of effective information security strategy outweigh the cost.

6.3 IMPLEMENTATION CHALLENGES

The major challenge envisaged is seeking EXCO's approval for the presentation of the findings and implementation of the preferred option in view of the recent happenings in the bank which involves the merging and acquisition by another bank.

6.4 CRITICAL SUCCESS FACTORS

ED Service Bank has approved the implementation of the option of choice - Adopting NIST Cybersecurity Framework. He encouraged it and specifically asked to be presented with a memo concerning the findings and recommendations to other business executives. The implementation of effective information security strategy to prevent e-fraud is a much welcome idea by the management and the business executives. Management is quite pleased that this can be initiated at a cost that is almost within routine expenses because the project prioritises cost effectiveness. At this point of the study, approval has been gotten to initiate the first phases of the implementation plan. Management has given the information security group the mandate to start a bank-wide information security awareness to all employees of the bank with immediate effect. The management specialised awareness session will start in mid-April, 2016 date will be agreed later. Budget has also been allocated for technical training of all staff whose jobs are related to information security to ensure adequate understanding of the adopted framework.

6.5 CONCLUSION

This chapter presented the implementation plan of the preferred option, budget, cost-benefit analysis, implementation challenges and the critical success factors.

The next chapter considers the researcher's reflections.

CHAPTER SEVEN

7.0 REFLECTIONS

7.1 INTRODUCTION

This chapter evaluated the research results against the researcher's expectations. It further assessed the dissertation against the researcher's initial execution plan and analyzed what went wrong, what turned out differently, and why. It also discussed the experiential knowledge the researcher gained from the entire dissertation process.

7.2 EVALUATION OF RESEARCH RESULTS AGAINST THE RESEARCHER'S EXPECTATIONS

The researcher expected the members of staff participated in the discussion and interview to be very responsive in the exercise but this was not the case as the researcher found it difficult to carry out the exercise. The researcher has to devise a means to get them participated through personal relationship and convincing approach. The participants were very interested in the research topic because it reflects one of the current issues in the bank. Before now, the researcher thought that technical security controls will be the main focus for the strategy to combat e-fraud, however the research shed more light on the strategy to align information security with business objectives by ensuring management commitment and buy in and using a framework that can be easily internalized to the bank.

7.3 ASSESSMENT OF THE DISSERTATION AGAINST THE RESEARCHER'S INITIAL EXECUTION PLAN

The researcher was able to come with the research topic and one-pager as earlier as possible with the hope of concluding the dissertation like two months before the deadline, however the paste were a little bit slower because of the researcher commitment to other projects and deliverables at work. The dissertation was eventually completed just before the due date.

7.4 ANALYSIS OF CHALLENGES

Even though the researcher plan adequately for the dissertation with a well though-out strategy, this was a bit thwarted by other job exigencies at work. The researcher was engaged in a project that took the researcher round some of the branches in the country in the bank. This affects the progress of the research as the target audience for the samples are staff in head office location. The researcher also found it difficult to agree on a date that will be convenient for data administration especially for the management staff involve because of their busy schedule.

Also, getting the honest participation of the team leads of various units who are supposed to be in charge of the management of information security was a bit difficult initially because they saw it as a form of audit to challenge how effective they are on their job's function.

7.5 EXPERIENTIAL KNOWLEDGE GAINED

The study revealed to the management on the best approaches to resolving the escalating e-fraud in the bank. The bank would be able to prevent e-fraud using information security strategy. The research work also served as an eye opener to the researcher. The researcher was able to review a lot of articles and journals on information security, electronic fraud, information security management, cybersecurity and how to protect e-fraud using information security management strategy.

The research work got more interesting with a knowing fact that a critical problem affecting an Organisation needed resolution. The knowledge gained cannot be overemphasized as it helped the researcher to have hindsight for problem analysis, recommendation and implementation. With the research work, the researcher had a better understanding of how to analyse problems that may arise in an Organisation using action learning.

BSN Action learning MBA had improved the researcher's management, organisational, writing and leadership skills greatly, though extremely very tasking in terms of intensive workshops, set meetings, unending research, and practical application of the knowledge acquired in more than two years it has lasted but it has imparted positively and turned around the researcher's department that did not align to business objectives as the bank now felt the need for IT Security & Compliance.

The following are the major learnings that the researcher acquired during this ALMBA journey.

1. The capacity to analyse an organisation, utilizing appropriate research techniques. This action, which included contrasting the researcher's findings and what has been documented in literature, empowered the researcher to watch the variance between best practices and what obtained in the researcher's organisation.
2. The researcher also had in-depth knowledge of the concept of Human Resources as a strategic business partner.
3. The researcher's knowledge of marketing was transformed through the BSN ALMBA. Amongst several other concepts, the researcher learnt about:

i. How to create raving fans
ii. Marketing and emotions
iii. The role of Branding
iv. How to manage customer relationships
v. How to gauge overall customer experience and what to do to improve same

4. The researcher's knowledge of operational management was enhanced. The researched enjoyed the workshop topics on Process Improvement topic such as lean six, total Quality Management. The researcher gained deeper understanding of project management principle. Concept of Lean Six to reduce waste and variation in a process arouse the researcher interest on further personal study on lean six sigma. The researcher is now lean six sigma black belt certified.
5. The financial management opened the researcher's mind and how to interpret financial statement, more knowledge on the concept of budgeting and deeper understanding of the concept of balanced score card and how to implement balance score card I researcher's environment
6. At the time of undertaking the workshop on information management, the researcher is the head, Information Technology (IT) Security and Compliance a unit under IT Group. The researcher is responsible for coordinating the governance, risk, control and compliance in the IT department. He interfaces with various departments in the bank whenever new IT assets (hardware or software) is acquired or developed. He also ensures that information security objective aligns with the bank's overall objective. The researcher gained further concept of information management and able to learn new approaches for helping people to adopt new technologies for their use, especially in business and the workplace.
7. The researcher's understanding of strategy formulation, business modelling, strategic planning, and other related concepts have also been enriched.
8. It is also important to note that this ALMBA changed increase the horizon of the researcher's and spark the researcher's interest in writing as currently, the researcher had been engaged as writers with two international bodies on matter related to information security.

7.6 CONCLUSION

This chapter presented the researcher's reflection on the entire dissertation process. It thus evaluated the research results against the researcher's expectations. It further assessed the dissertation against the researcher's initial execution plan and also analysed what went wrong, what turned out differently, and why. It also discussed the experiential knowledge the researcher gained from the entire dissertation process.

8.0 BIBLIOGRAPHY

ACI Universal Payments, Thought Leadership. Fighting Online Fraud: An Industry Perspective Vol3, 2014

Alhogail, A.R.E.E.J. and Mirza, A., 2014. A framework of information security culture change. Journal of Theoretical and Applied Information Technology, 64(2), pp.540-549

Behdad, M., Barone, L., French, T. and Bennamoun, M., 2012. On XCSR for electronic fraud detection. Evolutionary Intelligence, 2(5), pp.139-150.

Borrego, M., Douglas, E. P., & Amelink, C. T (2009), Quantitative, qualitative, and mixed research methods in engineering education. Journal of Engineering Education, 98(1), 53-66.

Brahma, SS 2009, 'Assessment of Construct Validity in Management Research', Journal Of Management Research (09725814), 9, 2, pp. 59-71, Business Source Premier, EBSCOhost, viewed 28 January 2016.

Calder, A. and Williams, G., 2014. PCI DSS: A Pocket Guide. IT Governance Publishing.

Chen, Y, Ramamurthy, K, & Wen, K 2012, 'Organisations' Information Security Policy Compliance: Stick or Carrot Approach?', Journal Of Management Information Systems, 29, 3, pp. 157-188, Business Source Premier, EBSCOhost, viewed 16 February 2016llek

Da Veiga, A. and Eloff, J.H., 2010. A framework and assessment instrument for information security culture. *Computers & Security*, *29*(2), pp.196-207.

De Haes, S, Van Grembergen, W, & Debreceny, R 2013, 'COBIT 5 and Enterprise Governance of Information Technology: Building Blocks and Research Opportunities', Journal Of Information Systems, 27, 1, pp. 307-324, Business Source Premier, EBSCOhost, viewed 10 March 2016.

Developing an Information Security and Risk Management Strategy (Part 1) by Ricky M. & Monique L. Magalhaes http://www.windowsecurity.com/articles-tutorials/intrusion_detection/developing-information-security-and-risk-management-strategy-part1.html (accessed February 21, 2016)

Developing an Information Security and Risk Management Strategy (Part 2) by Ricky M. & Monique L. Magalhaes http://www.windowsecurity.com/articles-tutorials/intrusion_detection/developing-information-security-and-risk-management-strategy-part2.html (accessed February 21, 2016)

Fabian A. E. (2003). Information technology in Nigerian banks: The limits of expectations. *Information Technology for Development.* Africa Regional Centre for Information Science, University of Ibadan, Nigeria, Vol. 10, 13–24.

Final version of NIST cybersecurity framework draws mixed reviews. Retrieved March 8, 2016 from http://searchsecurity.techtarget.com/news/2240214505/Final-version-of-NIST-cybersecurity-framework-draws-mixed-reviews

Flick, T., 2009. Hacking the smart grid. Black Hat USA Conf., Las Vegas, NV.

Freeman, EH 2007, 'Holistic Information Security: ISO 27001 and Due Care', Information Systems Security, 16, 5, pp. 291-294, Business Source Premier, EBSCOhost, viewed 9 March 2016

The Importance of Building an Information Security Strategic Plan by Brian Evans, 2015 https://securityintelligence.com/the-importance-of-building-an-information-security-strategic-plan/ (accessed February 21, 2016)

The Nigerian Cybercrimes (Prohibition, Prevention,Etc) Act, 2015

ISO/IEC 27001:2013, *Information technology — Security techniques — Information security management systems — Requirements*

ISACA Publication COBIT 5. *Frameworks for Information Security*, 2012

Istikoma, Bt Fakhri, N, Qurat-ul-Ain, & Ibrahim, J 2015, 'Information Security Aligned To Enterprise Management', Middle East Journal Of Business, 10, 1, pp. 62-66, Business Source Premier, EBSCOhost, viewed 16 February 2016.

International Organisation of Standards ISO 27001.*The ISO27001 Framework*. Retrieved April 24, 2015, from https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en2010

Kayworth, T. and Whitten, D., 2010. Effective information security requires a balance of social and technology factors. MIS Quarterly executive, 9(3), pp.2012-52.

Lei Shen. *Journal of Internet Law*. Dec 2014, Vol. 18 Issue 6, p3-6

Leonard Klie. CRM Magazine. *Data Security Should Be in Everyone's Job Description.* May 2015, Vol. 19 Issue 5, p32-36

Mathew J., Cindy M., and Beatriz J. (1999). Service quality in the banking sector: the impact of technology on service delivery. *International Journal of Bank Marketing,* 182-191.

Megafon, 2015, Indepth Interview. Available at http://uk.megafon.dk/331/in-depth-interview (Assessed on 28 December 2015)

NEFF 2014 Annual Report. Retrieved February 4, 2016 http://cbn.gov.ng/Out/2016/CCD/NEFF%202014%20Annual%20Report%20.pdf

NIST Cybersecurity Framework is Good and Bad. Retrieved March 8, 2016 from http://www.digitalcrazytown.com/2014/08/nist-cybersecurity-framework-is-good.html

NIST Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0, NIST.GOV (Feb. 12, 2014), available at http://www.nist.gov/cyberframework/upload/cybersecurityframework-021214.pdf

Payment Card Industry (PCI) Data Security Standard, v3.1. Retrieved January 17, 2016 from https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-1.pdf

Pironti, J.P., 2010. Developing an Information Security and Risk Management Strategy. ISACA Journal, 2, p.28.

Privacy Technical Assistance Center (PTAC). *Data Security: Top Threats to Data Protection* Dec 2011

Shon Harris, "*CISSP All in One Exam Guide*", 6th Edition, 2013

Stephen H. and Maeve C. (2013). *Management Information Systems for the Information Age,* 9th Edition, McGraw-Hill Companies, Inc., 1221 Avenue, New York, NY, 10020.

Sushma Mishra and Robert Morris (2011), Information Security Effectiveness: A Research Framework, *Issues in Information Systems*, Vol. XII No. 1, pp 246-255

The Cybersecurity Risk. Communications of the ACM. Jun2012, Vol. 55 Issue 6, p29-32

Tom Olzak, COBIT 5 for information security: *The Underlying Principles*. Retrieved February 25, 2016 from http://www.techrepublic.com/blog/it-security/cobit-5-for-information-security-the-underlying-principles/

Trochim, W.M. (2002). *Research Methods Knowledge Base*, 1-34.

Thomson, K.L., von Solms, R. and Louw, L., 2006. Cultivating an organisational information security culture. Computer Fraud & Security, 2006(10), pp.7-11.

Usman, A, & Shah, M 2013, 'Critical Success Factors for Preventing e-Banking Fraud', Journal Of Internet Banking & Commerce, 18, 2, pp. 1-15, Business Source Premier, EBSCOhost, viewed 4 February 2016.

Wallace Foundation, 2015, Workbook E: Conducting In-Depth Interviews. Available at http://www.wallacefoundation.org/knowledge-center/after-school/collecting-and-using-data/Documents/Workbook-E-Indepth-Interviews.pdf (Assessed on 28 December 2015)

Whitman, M. and Mattord, H., 2011. *Principles of information security*. Cengage Learning.

Whitman, ME 2003, 'ENEMY AT THE GATE: THREATS TO INFORMATION SECURITY', Communications Of The ACM, 46, 8, pp. 91-95, Business Source Premier, EBSCOhost, viewed 4 February 2016

Xia Zhao; Johnson, M. Eric. Managing Information Access in Data-Rich Enterprises with Escalation and Incentives. International Journal of Electronic Commerce. Fall2010, Vol. 15 Issue 1, p79-112

Xia Zhao; Ling Xue, Andrew B Whinston. *Journal of Management Information Systems*. Summer 2013, Vol. 30 Issue 1, p123-152

Young, R, & Windsor, J 2010, 'Empirical Evaluation of Information Security Planning and Integration', Communications Of The Association For Information Systems, 26, pp. 245-266, Business Source Premier, EBSCOhost, viewed 4 February 2016.

Zhang, S. and Le, F.H., 2013. An Examination of the Practicability of COBIT Framework and the Proposal of a COBIT-BSC Model. Journal of Economics, 1, p.5.

9.0 APPENDIX

9.1 RESEARCH TOOL – INTERVIEW SCRIPT

Interview Design Document

To be used for interview sessions with staff whose job's functions are related to the management of information security in the bank
Enterprise Bank Limited

Designed for use as part of the dissertation
Implementation of Effective Information Security Management Strategy to Prevent E-Fraud in Enterprise

By
Zechariah Oluleke Akinpelu.

S/N	Interviewee	Designation	Date	Location
1	Fabian Okonkwo	Team Lead IT Audit	10-Mar-16	143, Ahmadu Bello Way, VI
2	Promise Sunday	Team Lead, IS Control	14-Mar-16	143, Ahmadu Bello Way, VI
3	Shade Mojola	Team lead, IT Compliance	15-Mar-16	143, Ahmadu Bello Way, VI
4	Uyi Akhiosa	Team lead, eFraud	16-Mar-16	143, Ahmadu Bello Way, VI
5	Niyi Olalemi	Head, IT Risk	17-Mar-16	143, Ahmadu Bello Way, VI
6	Femi Komolafe	Team lead, Application & Database Security	18-Mar-16	143, Ahmadu Bello Way, VI
7	Benjamin Nnatuanya	Team lead, Network Security	21-Mar-16	143, Ahmadu Bello Way, VI

8	Okechukcku Njemanze	Head, IT Operation	22-Mar-16	143, Ahmadu Bello Way, VI
9	Peter Edeogu	Team lead, Systems and Unix Security	23-Mar-16	143, Ahmadu Bello Way, VI

Schedules (i.e Date and Time) is subjected to change following appointment bookings with the interviewee

S/N	Activity	Time Allotted (Minutes)	Remarks
1	Opening	2	**The researcher introduces the objective of the meeting which is to implement effective strategy to prevent e-fraud in the bank**
2	Question 1	3	**This include follow up questions**
3	Question 2	3	
4	Question 3	3	
5	Question 4	3	
6	Question 5	3	
7	Question 6	3	
8	Question 7	3	
9	Question 8	3	
10	Question 9	3	
11	Question 10	3	
12	Question 11	3	
13	Question 12	3	
14	Question 13	3	
15	Question 14	3	
16	Question 15	3	
17	Question 16	3	
18	Question 17	3	
19	Question 18	3	
20	Other Comments or Questions	5	
21	Total Time	61	

Requirements

Item	Remarks
Notepad and Pen	Researcher will bring his own
Recording Device	Researcher uses his smarphone

Interview Script	Prepared by researcher
Refreshment	Not Required

INTERVIEW Questions

Question 1: How is access control to systems, application and network in EBL handled based on each staff job's functions?

Question 2.What is the management perception of Information Security Management?

Question 3. How is the information security perceived by staff of EBL?

Question 4: Is there standard procedures or approvals before an IT change is made that will impact the bank information system?

Question 5: Is the network, host, and application(s) vulnerable to attacks from the internet or intranet which result in financial/reputational loss?

Question 6: Can malicious user easily access, modify, or destroy data or services within the system due to the current information security practices?

Question 7: Is there adequate technical control in place to protect the bank's network to prevent financial loss?

Question 8: Is Security Review and assurance part of business process and IT operational activities?

Question 9: Is there a strategy for Enforcement of Information Security in EBL?

Question 10: Is there frameworks that cover all aspect of Information Security Management.in EBL?

Question 11: Is EBL culture, ethics and behaviours reflect a secure IT environment?

Question 12: Are you adequately trained on Information Security Management principle as it relates to protection of bank's information asset?

Question 13: What is the rate of major breaches involving sensitive or confidential information for the past one year?

Question 14: What is the rate of stealing customers' data at rest or in motion for the past 3 months?

Question 15: What is the rate of malware and virus infection of sensitive data for the past one month?

Question 16: Has the bank suffered financial loss and reputational damage due to inefficient information security strategy?

Question 17: What can be done to ensure that management are accountable for Information Security Management Strategy?

Question 18: What measure can be put in place to prevent the recurring e-fraud in the bank?

9.2 DISSERTATION GROUP DISCUSSION SCRIPT

Group Discussion Design Document

To be used for group discussion for the management staff whose job's functions are related to the management of information security in the bank
Enterprise Bank Limited

Designed for use as part of the dissertation
Implementation of Effective Information Security Management Strategy to Prevent E-Fraud in Enterprise

By
Zechariah Oluleke Akinpelu.

Meeting Logistics

Target Meeting Date: Saturday, 24 March 2016

Target Start Time: 9.00am

Target End Time: 1.00pm

Proposed Location: Head Officer Ground Floor Meeting Room Enterprise Bank Ltd, Plot 21, Ahmadu Bello Way, Victoria Island, Lagos

Facilitator/Moderator: Zechariah Oluleke Akinpelu

Asst. Moderator/Time Keeper: Femi Komolafe

Strategy Session			
S/N	Participant	Designation	Location
1	Gboyega Dada	Chief Information Officer	143, Ahmadu Bello Way, VI
2	Louis	Chief Risk Officer	143, Ahmadu Bello Way, VI
3	Chuks Ekpunobi	Chief Compliance Officer	143, Ahmadu Bello Way, VI
4	Bukola Moradeyo	Chief Internal Auditor	143, Ahmadu Bello Way, VI
5	Daniel Adaramola	Chief Information Security Officer	143, Ahmadu Bello Way, VI
6	Ori Ogba	Group Head, Ebusiness	143, Ahmadu Bello Way, VI

Requirements

Item	**Remarks**
Notepad and Pen	Participants
Flip Chart	Available
White Baord	Available
Projector	Available
Business Model Canvas Paper	Available
Post-it Notes	Available
Laptop	Facilitator to bring his laptop
Focus Group Script	Prepared by Facilitator
Sound Recorder	Researcher's Samsung Smartphone (S5)
Markers	Available
Refreshment	Snack, Coffee, Tea:To be made available in the room and self serve

1. Call to order

1.1 After thanking the participants for coming, Zechariah called to order the Strategy Session 9am on Saturday 24th March, 2016 at the meeting room, Ground Floor, Enterprise Bank Ltd, 143, Ahmadu Bello Way, Victoria Island, Lagos, Nigeria.

2. Meeting Proper

2.1 The researcher welcomed the participants and introduced the objective of the meeting – to discuss how to implement of Effective Information Security Management Strategy to Prevent E-Fraud in Enterprise Limited

2.2 He explained that the session was important, because if not well articulated, the objective of preventing e-fraud in Enterprise Bank will not be achieved. He also noted that during the course of the session, all questions, comments, suggestions would be considered relevant, as all ideas are welcome.

2.3 The researcher urged the participants to switch off their phones or put it in silence so as to have little or no interruptions.

2.4 The Chief Information Security Officer – Daniel Adaramola thanked everyone for attending the meeting. He stressed the need to curb the escalating e-fraud in the bank by implementing effective information security management. In addition, he reiterated that this strategy session was an important one.

Group Discussion Scripts

S/N	Activity	Time Allotted(Minutes)	Remarks
1	Opening	2	The researcher introduces the objective of the meeting which is to implement effective strategy to prevent e-fraud in the bank
2	Question 1	15	This include follow up questions
3	Question 2	15	
4	Question 3	15	
5	Question 4	15	
6	Question 5	15	
7	Question 6	15	
8	Tea Break	30	
9	Question 7	15	
10	Question 8	15	
11	Question 9	15	
12	Question 10	15	
13	Question 11	15	
14	Question 12	15	
15	Other Contributions or Questions	20	
16	Appreciation and Closure	5	
17	**Total Time**	**237**	
18	Lunch		

DISCUSSION GROUP QUESTIONS

1. What is the current practice like in the Planning of Information Security in the bank?
2. How is the current Monitoring and Reviewing Process of Information Security like in the bank?
3. How is the current Maintenance and improvement of Information Security like in the bank?
4. What are the available information security related Documents and records in the bank?
5. How do the management view information security management in the bank?
6. Is the Top Management committed to the practice of information security?
7. What are the gaps in the planning of Information Security in the bank?
8. Has the bank's network, application and systems been infiltrated with Virus or Malware?
9. Has the bank been exposed to Hacking that lead to financial in the past two year?
10. What are the customer's (internal or external) complaints like on the unauthorized access or modification on their accounts?
11. What can be done to improve the existing information security strategy?
12. What are the controls to be implemented to prevent e-fraud?

9.3 EBL FRAUD STATISTICS AND UPDATES

1.1 Fraud Statistics and Updates

Summary of EBL Fraud cases are presented below;

Categorization of Fraud & Forgery Cases	No. of cases (Aug to Oct '14)	Fraud Amount August – Oct. 2014 (₦)	Potential Loss August to Oct (₦)	Fraud Amount Year to Date (₦)	Potential Loss Year to Date (₦)	Staff related Yr. to Date	Staff related cases Year to Date (₦)
Cash Suppression	2	2,239,600.00	0.00	5,757,940.00	520,000.00	11	5,757,940.00
Fraudulent Withdrawal	1	77,007,442.79	53,387,845.39	82,488,422.97	53,387,845.39	9	82,448,422.97
Computer Fraud/ATM	37	576,054,430.88	344,233,830.88	671,919,251.62	377,253,930.88	18	657,000,000.00
Account Opening Related	0	0.00	0.00	0.00	0.00	-	-
Robberies	1	3,715,000.00	3,715,000.00	6,713,000.00	6,713,000.00	-	-
Credit Fraud & Others	0	0.00	0.00	0.00	0.00	-	-
Total	**41**	**659,016,473.67**	**401,336,676.27**	**766,878,614.59**	**437,874,776.27**	**38**	**745,206,362.97**

- **The attempted frauds and irregularities investigated from August to October 2014 was about ₦659m out of which over ₦401.3m were successful. Computer fraud ranked first .**
- **Total fraud sum from January 2014 to date is ₦766.8m with a total sum of ₦745.2 (87%) linked to staff**
- **Staff related frauds are on the increase due to People and IT risks.**