An Investigation into the Critical Success Factors for E-Banking Frauds Prevention in Nigeria

By

Ahmad Kabir Usman

A thesis submitted in partial fulfilment for the requirements for the degree of Doctor of Philosophy at the University of Central Lancashire

October 2018

uclan
University of Central Lancashire

STUDENT DECLARATION FORM

I declare that while registered as a candidate for the research degree, I have not been a registered candidate or enrolled student for another award of the University or other academic or professional institution

I declare that no material contained in the thesis has been used in any other submission for an academic award and is solely my own work

Signature of Candidate :

Type of Award : **Doctor of Philosophy (PhD)**

School : **Lancashire School of Business & Enterprise**

ABSTRACT

E-Banking frauds is an issue experienced globally and continues to prove costly to both banks and customers. Frauds in e-banking services occur due to various compromises in security, ranging from weak authentication systems to insufficient internal controls. Although some security frameworks to address this issue of fraud have been proposed, the problem of e-banking fraud remains due to the inability of these framework to deal with organisational issues. With limited research in this area, the study sets out to identify the organisational Critical Success Factors (CSF) for E-Banking Frauds Prevention in Nigeria by applying CSF theory. A framework is proposed to help improve security from an organisational perspective.

The study adopted a mixture of philosophical paradigms which led to the triangulation of research methods; Literature Review, Survey and Case Studies. The Literature Review involved the synthesis of existing literature and identified potential CSF for frauds prevention in e-banking. A total of 28 factors were identified and a conceptual framework was proposed. A 5-point Likert scale survey questionnaire was sent to retail bank staff in Nigeria to rate the criticality of the factors. A total of 110 useable responses were received at a response rate of 23.9%. Similar interrelated factors were grouped using a Principal Component Analysis. Finally, case studies with 4 banks in Nigeria were carried out to deepen our understanding.

The study identified a total of 10 CSF which spanned across strategic, operational and technological factor categories. These included 'Management Commitment', 'Engagement of Subject Matter Experts' and 'Multi-Layer Authentication' amongst others. In addition, new CSF such as 'Risk-Based Transactional Controls', 'People Awareness & Training' and 'Bank Agility via Data Driven Decision Making' were identified. Finally, these CSF were grouped into an e-banking frauds prevention framework. This study is a pioneer study that extends theory to propose a CSF-based frauds prevention framework for banks in Nigeria.

ACKNOWLEDGEMENTS

Let me begin by thanking God for giving me the strength and health to carry out this research. There have been many people and organizations whose support have been essential for me to complete this journey. I will like to thank all the staff and other research students in the Lancashire School of Business & Enterprise, for always listening to my queries and providing feedback and support. I will particularly like to thank my supervisory team, Dr Mahmood Shah, Professor Yahaya Yusuf, Professor Mitch Larson, Professor Waqar Ahmed and Margaret Fisher for all the time, knowledge and guidance they have shared throughout the study period.

Let me thank all academics referenced within this thesis, as they have directly or indirectly contributed towards this research. Without the understanding of previous studies and theories, this research would have not been possible.

Finally, I will like to thank my wife, parents, all family and friends whom are too many to mention. I thank you all for your words of encouragement and support, all of which has led to the successful completion of this thesis.

Thank you.

PUBLICATIONS

Usman, A. K. and Shah, M.H., (2013). ‘Critical success factors for preventing e-banking fraud’. The Journal of Internet Banking and Commerce, 18(2), pp.1-14.

Usman, A.K. and Shah, M.H., (2013). ‘Strengthening E-banking Security using Keystroke Dynamics’. The Journal of Internet Banking and Commerce, 18(3), pp.1-11.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ACRONYMS

ATM	Automated Teller Machine
BRC	Board Risk Committee
BSI	British Standard Institute
BVN	Biometric Verification Number
CBN	Central Bank of Nigeria
CFA	Confirmatory Factor Analysis
CFF	Critical Failure Factors
CSB	Case Study Bank
CSF	Critical Success Factors
CSO	Chief Security Officer
CSV	Comma Separated Values
CV	Curriculum Vitae
CVV2	Card Verification Value 2
DES	Data Encryption Standard
DMZ	De-Militarized Zone
DNA	Deoxyribonucleic Acid
EBFP	Electronic Banking Fraud Prevention
EFA	Exploratory Factor Analysis
EMV	Europay, MasterCard and Visa
FFIE	Federal Financial Institutions Examination
GDP	Gross Domestic Product
HR	Human Resource
HTTPS	Hypertext Transfer Protocol Secure

IBM	International Business Machines
ICT	Information & Communication Technology
ID	Identity
IFRS	International Financial Reporting Standards
IP	Internet Protocol
IS	Information Systems
ISO	International Standards Organisation
IT	Information Technology
KMO	Kaiser-Meyer-Olkin
KPI	Key Performance Indicator
KSF	Key Success Factors
KYC	Know Your Customer
MIME	Multipurpose Internet Mail Extensions
MIS	Management Information System
NeFF	Nigerian Electronic Fraud Forum
NIBSS	Nigerian Inter Bank Settlement System
OTP	One Time Password
PA DSS	Payment Application Industry Data Security Standards
PC	Personal Computer
PCA	Principal Component Analysis
PCI DSS	Payment Card Industry Data Security Standards
PIN	Personal Identification Number
POS	Point of Service
RCA	Root Cause Analysis
SMS	Short Message Service
SPSS	Statistical Package for the Social Sciences
SWOT	Strengths, Weaknesses, Opportunities and Threats
TPB	Theory of Planned Behaviour
UK	United Kingdom
URL	Universal Resource Locator
US	United States of America
USD	United States Dollar

CHAPTER 1: INTRODUCTION

1.1 Introduction

This chapter introduces the scope of the research for this thesis. It describes the background, methods and tools employed. The introduction provides the context of the research which is covered in more detail within subsequent chapters.

The research described in this thesis is titled ‘An investigation into the Critical Success Factors (CSF) for E-Banking Frauds Prevention in Nigeria’. This chapter begins with providing some background in e-banking and security to set the scene. The first section outlines how electronic banking has revolutionised financial institutions, payment systems and businesses. It then proceeds to highlight existing security challenges and describe how security measures have continually developed to address the threats associated with e-banking services, specifically relating to fraud.

The problem statement is presented and leads into the research questions. The detailed aims, objectives, research questions and methodological issues related to the empirical part of the research are also covered in this chapter. The chapter ends by outlining the content of all subsequent chapters of this thesis for the ease of readability and clear flow of argument.

1.2 Research Context

The adoption of E-banking services has revolutionised how financial transactions are carried out globally. The increasing popularity and accessibility of the internet has been an important factor as it provides the backbone for e-banking services to take place. Poong *et al.* (2009) highlighted that the internet enables people worldwide to carry out commercial activities whenever and wherever they desire. Historically, e-banking services required a PC, modem and software provided by the financial services vendors (Kamel, 2006). However, growing availability of the internet and technology have led to increased availability of electronic banking services. E-banking is the automated delivery of new and traditional banking products and services directly to customers through electronic mediums allowing customers to access their accounts, transact business, make enquiries and receive prompt responses from banks (Parisa, 2006). The scope of e-banking services includes Online Banking, Automated Teller Machines (ATM), Mobile Banking, and Short Messaging Service banking (Kavitha, 2017). In summary, an electronic service which enables banks and customers to send and receive instructions is deemed to be an e-banking service.

With the growing patronage of e-banking services, some of the known factors capable of hindering its growth must be addressed. Security concerns are of greatest importance for the adoption of e-banking services (Angelakopoulos and Mihiotis, 2011). In 1998, Roberds (1998) highlighted that the incentives for fraud increase in scenarios where transactions can be made in large amounts, cannot be effectively verified at the point of sale and when issuers of payment claims bear the costs of fraud. E-Banking offers most if not all these incentives, therefore attracting fraudulent activity and security challenges. Tsai *et al.* (2010) also explained that the dynamic nature of technology and e-banking presents unique security challenges require novel solutions. More recently, researchers highlight the frequency and sophistication of cyber-attacks as one of the challenges in securing e-banking services (Camillo, 2017). Therefore, there is need for banks to continually ensure that their e-banking channels are secure taking into consideration the dynamic nature of technology and threats.

E-Banking fraud continues to dominate fraud losses globally. In the UK, 98% of financial fraud losses are experienced via payment card or online banking fraud (Financial Fraud Action, 2016). However, the statistics also show that there has been improvements in preventing fraud over e-banking with over 60% of the attempted fraud cases now being detected and prevented. In Nigeria, the country has witnessed an overall reduction in fraud losses from 2015 to 2016 despite its year on year increase in the adoption of e-banking services (NeFF, 2017). Nevertheless, lapses in security leading to fraud are still costing banks and customers significant amounts of losses, both financial and non-financial.

The most common responses from organizations to security breaches are to utilise information technology (Rhee *et al.*, 2009; Maçada and Luciano, 2010). However, this does not cater to the whole spectrum of risks involved with e-banking services. For example, its impact is limited when employee negligence or destructive behaviour comes into play. Banks must ensure that they have adequate security to prevent existing threats and adapt to the continuously evolving and new threats to their data and payment systems, all to prevent fraud. These issues are examined in the context of CSF in e-banking services during this research.

1.3 Challenges in E-Banking Security

The proliferation of E-Banking Services worldwide has made securing e-banking mediums become more imperative. Nigeria is known as the "Giant of Africa" due to the country having the largest population and largest economy in Africa (Falola *et al.*, 2018). This presents huge potential for banks and customers to benefit from e-banking services. Banks have already made significant investments in technology and their investments have been corroborated by users' acceptance despite the concerns with security (Oni and Ayo, 2010). Some of the benefits associated with e-banking services have started to yield dividend by reflecting positively in banks' business performance results (Agwu, 2018). However, fraud over e-banking mediums remains an issue, and overcoming existing e-banking security challenges may help yield greater levels of adoption.

In Nigeria, the types of fraud that are commonly experienced by financial institutions include sales fraud, purchase fraud, cheque payment fraud and ATM fraud (Benjamin and Samson, 2011). Tade and Adeniyi (2017) investigated into ATM fraud and found customers sharing their details with loved ones, physical attacks and card cloning were all challenges being experienced in Nigeria. Some of the strategies employed by fraudsters in Nigeria include collaborating with security agents and bank officials to obtain information which they then feed into their local and international networks (Aransiola and Asindemade, 2011). Adetiloye *et al.* (2016) investigated into fraud prevention in banks and found that internal controls had historically been an area of weakness. It was highlighted that low remuneration of employees, lack of security awareness, and the increasing adoption of contract staff to reduce costs were all factors which contributed to the occurrences of fraud.

Fraud is not unique to the financial services industry but to many others too. Research to prevent fraud has spanned various industries. For example, Tatiana (2017) investigated into fraud prevention of government auditors whilst Prenzler (2016) studied fraud prevention in welfare claims. Other examples include research on value added tax fraud by Hoza and Wojcicki (2017) whilst Epstein (2017) researched into fraud in healthcare payments. These studies were carried out across different countries, indicating that fraud is a global issue. Research specific to e-banking fraud prevention (EBFP) remains not only limited but primarily geared towards technological advancements rather than considering factors spanning people, processes and technology.

Although fraud remains a menace, some countries are making progress with statistics showing a decrease in losses in recent times. This can be attested to by the figures provided earlier in this chapter with respect to frauds in the UK and Nigeria. This provides an indication that the banks preventative measures are yielding some dividend in relation to the security measures which they are implementing.

1.4 Problem Statement

Although Nigeria has witnessed its e-banking services gaining a lot of attention due to the advantages, there are still many customers unwilling to adopt e-banking- services due to the risk involved or lack of trust (Arora and Kaur, 2018). It has been found that there is a significant positive relationship between perceived security and e-banking adoption (Salimon *et al.*, 2017). This indicates that strengthened e-banking security to prevent frauds may lead to greater levels of adoption. In addition, ensuring that the trust is maintained with customers via secured processing of their transactions has also been identified as beneficial for the retention of customers' using e-banking services (Adeqoye and Ayo, 2010). Agwu and Carter (2018) also call for the improvement of security for e-banking services to help increase adoption rates. Worryingly, only 42% of Nigerian banking customers use e-banking services and these low rates are partially attributed to the need to reinforce customer trust (KPMG, 2017). This further indicates that there is an opportunity to substantially increase the levels of e-banking adoption in Nigeria.

Despite the effort banks have made to secure their e-banking services, large annual losses continue to be associated to fraud over e-banking mediums. In 2017, it was found that although fraud had decreased over some e-banking mediums, others had experienced an increase when compared to the previous year (NeFF, 2017). This indicates that fraud continues to be a problem for the banks in Nigeria. In order to address the menace of e-banking fraud, banks need to continuously secure their services by implementing appropriate security measures. There is an argument to suggest that no single solution can address the menace of electronic fraud (Herley and Van Oorschot, 2012). There is rather a need for a combination of measures whose effectiveness tends to diminish over time due to fraudsters continuous pursuit for loopholes and intrusions. This in addition to the continuous annual losses to fraud indicate that fraud prevention is an issue which requires continuous attention.

An extensive literature review revealed a shortage of in-depth research in e-banking frauds prevention which did not primarily focus on technology. Numerous studies focus on the technical aspects of IT security such as authentication systems and biometrics. On the other hand, there are studies that seek to understand behavioural decision making of customers and criminals. These all are important but do not proffer a holistic view on how to prevent fraud which should span across both technological and non-technological issues.

This research sets out to identify the CSF required to prevent E-Banking Fraud and propose a framework for banks. To achieve this, several approaches were considered which included Cost/Benefit Analysis, CSF, Key Performance Indicators and SWOT Analysis, amongst others. The Key Performance Indicator (KPI) system offers a means of investigating strategic issues and providing executives with the information they require (Rockart, 1979). The Cost/benefit analysis, also known as the Benefit/ Cost framework is a framework that reviews the trade-offs between costs and benefits with the view to decide on the best cause of action (Yung-Cheng *et al.*, 2010). The purpose of the SWOT (Strengths, Weaknesses, Opportunities and Threats) framework is to identify key issues for each category and facilitate a strategic approach. These theories are covered in more detail within Chapter 2 of this thesis.

CSF was introduced by Rockart in 1979 and is defined as the limited number of areas in which if they are satisfactory, will ensure successful performance (Rockart, 1979). The CSF theory is used in many modern information systems research. For example, Bobbert and Mulder (2015) applied the theory to identify factors suitable for information security whilst Humphrey (2017) identified CSF to improve security incident reporting. The CSF theory has evolved over the years as originally there was a lot of focus on identifying the list of CSF. Today, more meaningful information is derived such as rating the factors criticality, understanding correlations, dependencies and other useful information. CSF theory places emphasis on the utilisation of existing research and experiences to determine organisational factors. CSF was adopted for the study and justification on its selection, and how the study overcame the limitation of only providing a list is given later within this chapter.

1.5 Research Aims & Objectives

This research aims to investigate organisational factors that are critical for banks to prevent e-banking frauds and understand how those factors can be implemented so that they can be considered during strategic planning. The scope of e-banking services involves all electronic services provided by banks to its customers as further outlined in section 1.2. The objectives of the research are as follows:

- To investigate into the CSF of EBFP in similar contexts using a literature review
- To identify and validate the CSF for EBFP in Nigeria
- To propose a CSF based framework for preventing e-banking frauds

To be able to achieve the research objects, the following research questions were identified for the study:

1. What are the security challenges' in relation to fraud that banks experience whilst offering e-banking services?
2. What are the factors that have been employed that have successfully contributed to preventing fraud?
3. Are there variations with regards to the perceptions of criticality for the factors that prevent e-banking fraud between stakeholders of different demographics?

4. Which of the factors are the most critical in ensuring the successful prevention of e-banking fraud?
5. How do banks achieve the identified CSF to prevent e-banking frauds?

The findings will help banks and regulators build more effective fraud prevention strategies and align them with their organisational strategies. This research provides guidance on the security measures that e-banking fraud prevention strategies should adopt. To achieve this, existing security strategies and fraud prevention measures were thoroughly evaluated to understand their suitability, effectiveness and limitations.

1.6 Research Methodology

Although CSF theory originally focussed on refining the information needs of executives, there had also been reference to its usefulness for strategic planning in information systems or technology (Bullen and Rockart, 1981). More recently, the CSF theory has found its way into many information, business and technology planning methodologies (Caralli *et al.*, 2004). Both quantitative and qualitative research methods can be used to identify CSF. Methods previously employed for CSF research includes literature reviews Alnatheer (2015), case studies Caralli *et al.* (2004), surveys Lopes and Oliveira (2015), interviews Micheni (2017) and the Delphi method Humphrey (2017) amongst others. Shah and Siddiqui (2006) concluded that the survey approach is the most commonly used method for the identification of CSF. However, other studies have shown that case studies and interviews are also popular methods utilised.

For the purposes of this research, methodological triangulation was adopted. The research process involved the identification and verification of the factors until a conclusive set of CSF for e-banking frauds prevention had been achieved. The research approach adopted was to primarily use the literature review and survey for CSF identification whilst leveraging case studies to gain deeper insight into the identified factors. This aligns similarly to previous CSF research by De Sousa (2004) cited in (Amberg *et al.*, 2005). To achieve the research objectives, the research methodology was conducted in three phases, and in the following order:

- Phase 1: Systematic Literature Review
- Phase 2: Survey
- Phase 3: Case Study

A conceptual framework was proposed and refined across the phases of the research. Chapter 3 of this thesis provides further details on the research methodology and figure 3.1 provides a summary of what was covered during each phase.

1.7 Justification on CSF Theory Selection

The CSF theory was chosen for this research as it is an appropriate means of determining the important measures that will help towards preventing e-banking frauds. Rockart (1979) explains that one of the benefits of adopting the CSF theory is that it not only helps management determine the relevant CSF, it also ensures that the CSF receive continuous scrutiny. As there are numerous measures which banks can take to prevent fraud, the CSF theory helps identify the factors that should be treated with highest priority. The study primarily focussed on internal factors that organizations can control.

One of the limitations of the CSF theory is that it can be seen to produce a list, which is of limited value. Such a list makes it difficult for management to translate CSF and define their concrete needs (Boynton and Zmud, 1984). This research attempts to overcome this limitation by synthesising preventative organisational factors and proposing a conceptual framework which consists of e-banking fraud prevention factors. Additionally, the framework provides practical concepts and activities for organisations to achieve the critical factors. This is similar to previous CSF studies (Caralli *et al.,* 2004; Ngai *et al.,* 2008) in which each of the factors are presented with descriptions and activities for deeper understanding. Hence, offering insights on how the CSF can be achieved. Additional benefits of the CSF theory are captured in the Literature Review, Chapter 2 of this thesis.

CSF theory have been used frequently in academia, and literature has shown that there are different ways in which it can be applied. Alnatheer (2015) adopted CSF theory to help identify factors to support creating an information security culture. Humphrey (2017) used CSF theory to specifically identify the factors that help improve security incident reporting. Javadin *et al.* (2015) covered a broader range of scope as their study investigated into the CSF for effective information security management. Miranda *et al.* (2014) employed the use of CSF theory to propose a framework for e-learning. Therefore, the theory is popularly used in research to address research problems. A review of previous studies highlighted that the CSF theory has been applied to both e-banking and security related topics previously, although not in the context of this research.

1.8 Originality & Contribution

The CSF theory has not previously been extended in the context of e-banking frauds prevention. Given the dynamic nature of e-banking services and security threats, the study provides a unique synthesis of factors that banks should consider during their strategic planning to prevent frauds and incorporate into their organisations. The originality of this research is that it takes a well-known and proven theory and applies it to propose a framework for EBFP. The study goes beyond the identification CSF, but also provides further insight for each of the factors taking cognisance of theory relating to the application of organisational CSF.

This unique study also addresses the gaps of previous research where there has been a tendency to focus on technology for preventing fraud, excluding other organisational factors. Although, the importance of technology cannot be over emphasised, studies have shown that non-technological issues can be just as important (Alfawaz *et al.*, 2010). This study therefore adopts the CSF theory to encapsulate both technological and non-technological factors for EBFP.

Finally, the success of the research may help promote research in developing countries where it is already known to be lacking (Yeoh *et al.*, 2008). This became further evident during the literature review phase of the study where it was found that empirical research in Nigeria, within the context of this study is limited.

1.9 Thesis Outline

This thesis is structured into seven chapters, each one addressing a distinct point in this research. The outline follows the steps that were involved in the research starting from identifying the research questions, developing the research methodology, data collation, analysis, and finally drawing conclusions. The figure below depicts the thesis outline by chapter:

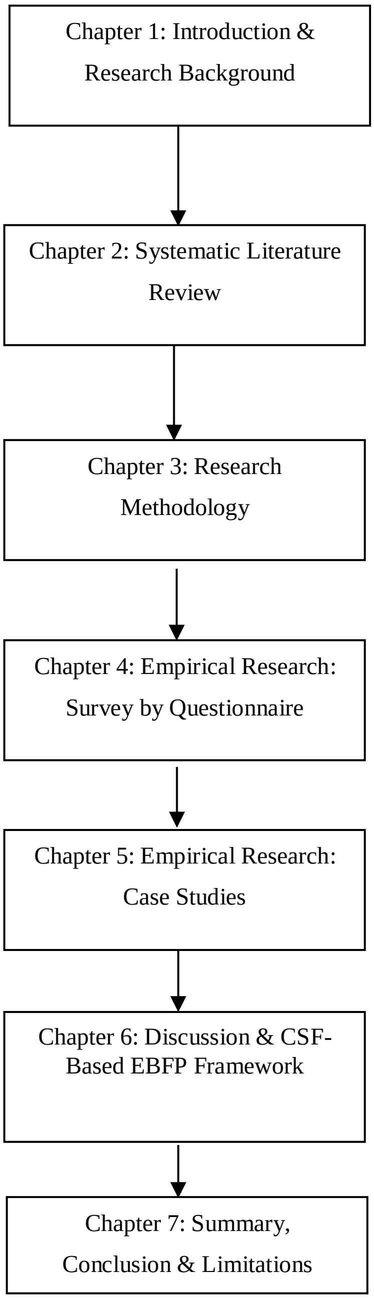

Chapter 1: Introduction & Research Background
Chapter 2: Systematic Literature Review
Chapter 3: Research Methodology
Chapter 4: Empirical Research: Survey by Questionnaire
Chapter 5: Empirical Research: Case Studies
Chapter 6: Discussion & CSF-Based EBFP Framework
Chapter 7: Summary, Conclusion & Limitations

Figure 1.1: Thesis Outline

CHAPTER 2: LITERATURE REVIEW

2.1 Introduction

The world has experienced a significant transformation in banking operations due to the increasing influence of Information and Communication Technologies (ICT) and the proliferation of the Internet. Banking institutions are embracing e-b anking solutions to further improve customer service and increase their reach to the customers and transparency in the system, but fraud threats remain a challenge. This research set out to investigate the CSF for e-banking fraud prevention. To achieve this, e-banking fraud and existing research on fraud prevention needed to be understood. A review of literature both globally and in the Nigerian context was carried out to understand the challenges and measures employed to address them.

E-banking fraud is a global issue. Financial Fraud Action (2016) reported that in the UK, fraud losses on credit/debit cards had risen in value. However, these losses do overshadow some of the progress that has been made. For example, although the fraud losses had increased in value, the percentage of losses compared to the total value of e-banking transactions had decreased. This has been attributed to improved e-banking security. Nigeria has also experienced large losses due to fraud, but more recently the banks have experienced improvements in securing their electronic channels. For example, there was a significant decrease of 63% of actual losses between 2014 and 2015 and the trend continued with a 2.65% decrease in 2016 compared to the previous year (NeFF, 2017). Whilst there have been improvements in fraud prevention, there is still the need to consolidate the effective security measures to help organisations further minimise e-banking fraud.

This section will review, summarise and comment on past research, their methodologies and limitations. The document will proceed to introduce the e-banking environment, theory adopted for the research and proposes CSF for EBFP based on the findings of the literature review.

2.2 Literature Review Framework

A literature review is an objective and thorough summary and critical analysis of the relevant, available research and non-research literature on the topic being studied (Hart, 1998). For this study, traditional and systematic literature review types were considered. The researcher opted to use a systematic literature review and considered e-banking fraud and other electronic fraud or security related literature. A systematic literature review "is a means of evaluating and interpreting all available research relevant to a particular research question, or topic area, or phenomenon of interest" (Budgen and Brereton, 2006, p.1051). Therefore, ensuring thorough coverage of pertinent literature using a systematic approach. Kitchenham (2004) argues that if studies give consistent results, systematic reviews can evidence that the phenomenon is robust and assist with the generation of new hypothesis. The systematic literature review approach was selected as it offers a more structured means of establishing whether findings related to e-banking fraud prevention are consistent and can be generalised compared to using a traditional literature review.

The benefits of using a systematic literature review is that it is a repeatable method for identifying, evaluating and synthesising existing literature (Okolie and Schabram, 2010). In contrast, standard literature reviews may not be repeatable and may vary in terms of how the literature is analysed. Using a systematic approach also encourages transparency as it outlines the boundaries of what is in and out of scope for the review. Additionally, the approach helps protect against potential bias such as the selection of research papers that support the researcher's beliefs (Booth *et al.*, 2016). Similarly, Mulrow (1994) also suggests that systematic reviews limit bias and may improve the reliability and accuracy of conclusions. Systematic reviews are known to require considerably more effort compared to traditional literature reviews (Kitchenham, 2004). However, given the aforementioned benefits of the systematic literature review, the researcher adopted it as a more suited approach compared to traditional literature reviews.

The literature review was carried out in 3 phases in accordance with the guidelines of (Brereton *et al.*, 2007). These were:

1. Planning the review: This included specifying the research question, key words and then developing the review protocol

2. Conducting the review: This phase involved identification of the research literature, selection of the primary studies, data extraction and synthesis.
3. Reporting the review: This involved evaluating the literature and reporting the findings.

Conceptual boundaries of the review were defined to help achieve the objective of the review but also ensure clarity of the review scope. The previous chapter had outlined the research objective which is to investigate into the organisational factors that are critical for banks to prevent e-banking frauds. To achieve this, the literature review question was set as: What are the factors that have successfully contributed to preventing fraud?

The review of literature was primarily reliant on electronic sources which included access to journals, articles and other sources of knowledge such as e-books. The literature sources were limited to those that were found from the 7 databases explored which included Business Source Complete and Science Direct, amongst others. The databases were selected due to their suitability for identifying literature related to the topic and the full list of databases explored are available at Appendix A of this thesis. Finally, literature boundaries were defined along with the time period of when literature had been published. The restriction of literature to specific date ranges for their inclusion criteria is common for systematic literature reviews (Okolie and Schabram, 2010). For this study, the search range spanned a 15-year period. This was required given the limited research in the area of e-banking fraud prevention.

Each of the databases searched using a list of key words to focus on relevant literature. Appendix A of this thesis provides information on key words used during the search. After the literature was identified, they were downloaded and imported into a reference management software. The screening process entailed removing duplicates and any literature that fell outside of the boundaries of the defined time period. The next step involved reviewing abstracts to ensure relevance of the remaining literature. In some cases, an additional activity of reviewing the body of the literature was necessary where suitability of the literature could not be ascertained from solely the abstract. After these steps had been taken, a total number of 103 papers made the final sample list for further analysis.

Once the sample of 103 had been obtained, the findings of the studies were synthesised bringing together fraud prevention measures. The researcher captured this information in a spreadsheet to help group the factors into categories. Additionally, similar factors were grouped together and those that had occurred in multiple literature were identified. The output of the review was a synthesised set of factors that had been reported as effective in preventing fraud. Further details are also covered in the research methodology chapter of this thesis.

2.3 E-Banking Overview

2.3.1 E-Banking Introduction and Background

E-Banking services are the banking class of services that can be offered by a bank to individuals and companies through electronic means via a fixed or mobile telephone and Internet (Ratiu *et al.*, 2011). Banks now use the internet as a means of offering their services and receiving instructions from customers (Krishnan, 2017). E-Banking can also be described as a means of using technology to send and receive instructions with financial institutions where an account is held (Prakash and Malik, 2008). Given that internet technology has evolved considerably over the years, newly developed e-banking services now differ considerably from older systems (Khan and Mahapatra, 2009). For example, mobile banking has introduced a greater level of convenience for customers allowing them to carry out many transactions that would have previously involved logging into internet banking with a personal computer or even visiting an ATM. Additionally, it also provides customers with the ability to authorise transactions using a point of service device in real-time.

Historically, the first electronic ATM was developed in 1967 by Barclays Bank at Enfield Town in North London and in 1968, the networked ATM was pioneered in Dallas and Texas (Karamala and Anchula, 2011). The first cash dispenser built by Luther George Simjian had been installed since 1939 but was removed 6 months later due to the lack of customer acceptance, partly due to security perceptions. It wasn’t until 20 years later that

ATM’s were re-introduced (Karamala and Anchula, 2011). This highlights the potential impact that perceived lack of security can have on e-banking services.

2.3.2 Drivers & Benefits of E-Banking

Major drivers for the introduction of online banking were identified as a means of improving customer services to bank customers and reduce banks operating costs. It has been proved that the online banking channel is the cheapest delivery channel for banking products (Pikkarainen *et al.*, 2004). Mihalcescu *et al.* (2008) agrees with this statement highlighting that e-banking transactions are much cheaper than branch or telephone transactions. Tuchila (2000) categorised the advantages of online banking into 3 categories; improved market image, reduced transaction costs and increased market penetration.

From a customer perspective, convenience is one of the major benefits. Raja (2012) highlights round the clock banking, convenience, speed and range of services that can be accessed as some of the benefits. Customers no longer need to visit their banks for transactions as they can be done in the comfort of their homes or in transit. Thus, e-banking offers benefits for banks, customers and investors (Cheng *et al.*, 2006). Other benefits can include improved relationships with suppliers, quick delivery of products and services and the reduced risk of data entry related errors (Shah, 2009). Ajayi and Enitilo (2016) found that the introduction of e-banking services in Nigeria increased competition in the industry and reduced customer waiting time for bank transactions.

Undoubtedly, there are many advantages of using e-banking services for banks and customers. However, there are also challenges with respect to maintaining security and privacy to avoid misuse. Salimon *et al.* (2016) highlighted that lack of trust by customers prevent the adoption of e-banking services. It is therefore necessary to provide adequate security features to ensure the integrity of the transactions and instil confidence to its users (Ganesan and Vivekanandan, 2009). Kumar and Gupta (2009) presented a similar argument after their study identified transaction security as a CSF for enabling banks to move into an e-banking driven branchless model.

2.3.3 Nigerian Banking Industry

As the case study was carried out in Nigeria, a high-level background of the banking industry is included to help readers with the context. Nigeria is a country of over 185 Million people and a GDP of over $400 billion USD (World Bank, 2017). Despite this, over 46% of Nigerian adults don't have access to financial services as at 2010 (CBN, 2012). There has historically been a gap in the financial services infrastructure and service productivity compared with more developed countries. Of recent, e-banking has brought about an opportunity to address the gap in infrastructure and expand the reach of banks and payment systems.

Nigeria is recognized to be a late entrant to ICT especially when it comes to financial systems. After a slow start to e-banking in Nigeria, adoption in e-banking services have begun to gradually increase. Although there has been a steady increase in the use of e-banking services, Nigeria has historically been a cash-based economy (Ayo and Ukpere, 2010). In a bid to overcome the challenges associated with this, the Nigerian government has taken several steps to encourage the use of e-banking in the country. The Central Bank of Nigeria (CBN), which is the regulatory bank first introduced 'e-money' to Nigeria in the 1986 Monetary and Policy (CBN, 2016a). CBN then introduced its e-banking guidelines in 2004 to help improve the countries payment systems. This was a clear indication of the government's intent in transitioning to a cashless economy.

To further encourage the transition to e-banking services and protect the interest of customers, CBN plays a key role in ensuring banks implement adequate security measures. This is achieved by them defining electronic banking security guidelines which include the minimum security requirements that banks must implement before offering e-banking services. Nevertheless, banks are also actively securing their channels knowing the importance of protecting their customers and their reputation. The combination of this has led to improved e-banking fraud prevention in the Nigerian banking industry.

2.4 E-Banking Security Challenges

E-banking challenges experienced globally relate to security fears, cultural barriers, limited internet access and legislation (Masocha *et al.*, 2011). However, it has been reported that security concerns are of greatest importance (Angelakopoulos and Mihiotis, 2011). Financial services and organisations suffer yearly losses through crimes such as online banking, cheque and card fraud (Adams, 2010). Inadequate security potentially leads to financial losses, punitive measures by regulators and negative media publicity. E-banking services therefore contain risks that must be mitigated to instil and maintain customers' trust. T challenges associated with e-banking security which may lead to fraud are discussed below.

Dynamism of E-Banking Services

Managing the risk associated with fraud as well as diminishing its impact is an important issue that faces financial institutions as fraud techniques have become more advanced with increased occurrences (Adepoju and Alhassan, 2010). More so, the rapid advances in technology has introduced an increase of tools that can be used to carry out unauthorised behaviours (Alfawaz *et al.*, 2010). Hence, there is the need for careful management and continuous improvements in security to prevent fraud (Giles, 2010).

Lack of Strong Authentication Systems

The common use of the same passwords for many services increases the vulnerability whenever such information is stolen. This coupled with increasing cyber security threats such phishing and hacking all contribute towards weakened authentication systems. Researchers have emphasised the need for additional security measures to confirm people's identity (Moskovitch *et al.*, 2009). This coupled with the challenge of people compromising their PIN further weakens authentication systems (Raja, 2012).

People Compromising Security

It has been frequently mentioned that people are the weakest link in security chains (Sasse and Flechais, 2005). The management and implementation of security is done by people (Della-Libera *et al.*, 2002). Consequently, bank employees and customers can both be seen as weak links. In some cases, internal staff are knowingly involved in compromising security to carry out fraud. Strategies employed include collaboration with security agents and bank officials who work with local and international networks (Aransiola and Asindemade, 2011). Therefore, bank staff present an immediate and constant threat to e-banking services and its users. Myyry *et al.* (2009) indicated that the majority of security issues are due to employees violating or neglecting their organisations security policies. To counter this, it has been suggested that banks make customers aware of the risks associated with e-banking so that they follow prescribed security guidelines (Krishnan, 2017).

Allocation of Fraud Losses

Another factor contributing to the incidences of fraud is the allocation of losses. This defines who should bear the costs in the event of fraud. Costs can be allocated to the bank, seller or buyer. There is a belief that the distribution of the losses across all 3 options may be the best option as it affects the incentives to commit fraud (Roberds, 1998). All parties may take more precaution with the knowledge that any occurrence of fraud will impact them directly. However, there is an argument that suggests victims are commonly not able to recover the funds that they have been defrauded of (Virgo, 2007). Therefore, the allocation of losses may not have much impact after all.

The above highlights some of the pressing challenges experienced with e-banking security. These challenges may all lead to the menace of fraud. The consequences of fraud are not only financial but also includes loss of trust and inconvenience to the parties involved. Examples include the need for the cancelation of cards, freezing accounts and completing large volumes of paperwork. Thus, the repercussions of fraud are numerous.

2.5 E-Banking Fraud

Although there is no single accepted definition of fraud, it relates to wrongful or criminal deception that results in financial or personal gains (Matthew *et al.,* 2013). Benjamin and Samson (2011) defined fraud as the general manipulation or retention of information with criminal intent to deprive another party or parties of privileges, rights, or materials they posses. Dagogo and Ngerebo (2018) explains that there are two classes of fraud, institutional and socio-environmental. Institutional fraud is traceable to the internal environment of the bank whilst socio-environment are influenced by the society and environment. Card fraud is one of the most common fraud types in e-banking because cards can be used to carry out transactions physically using payment devices such as Automated Teller Machines (ATMs), and remotely where card data can be used to transact over the phone or internet. Therefore, fraudsters do not need to be physically present to defraud customers (Gates and Jacob, 2009). The diagram below provides a summary of card fraud losses worldwide from 2010 to 2018.

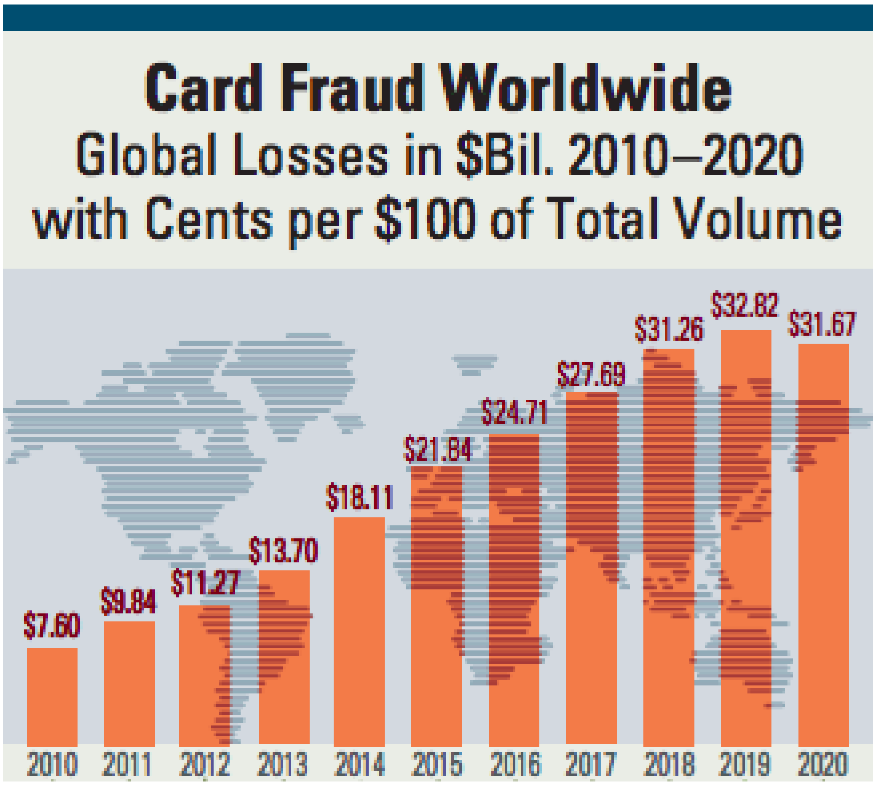


Figure 2.1: Worldwide Card Fraud Losses (Nilson, 2016).

The diagram highlights the extent of losses due to card fraud alone up until 2015. The projections for the years ahead suggest that these figures are expected to further rise with a decline by 2020 due to upgrades of ATMs to align to the Europay, Mastercard and Visa standard. Its anticipated that improved methods to prevent fraud via card not-present transactions will further help prevent fraud. More recently, Siddiqui and Qureshi (2017) project that online payment fraud will reach $25.6 billion, which is a lower figure than projected in figure 2.1 and may be due to the growing effectiveness of preventative measures. However, both projections highlight that fraud losses in 2020 will be more than what they are at present. The projection of large annual losses is a cause for concern for banks and customers, highlighting the risks associated with offering and using e-banking services. This also reiterates the importance of e-banking fraud prevention and the potential impact if effective measures can be put in place to minimise such losses.

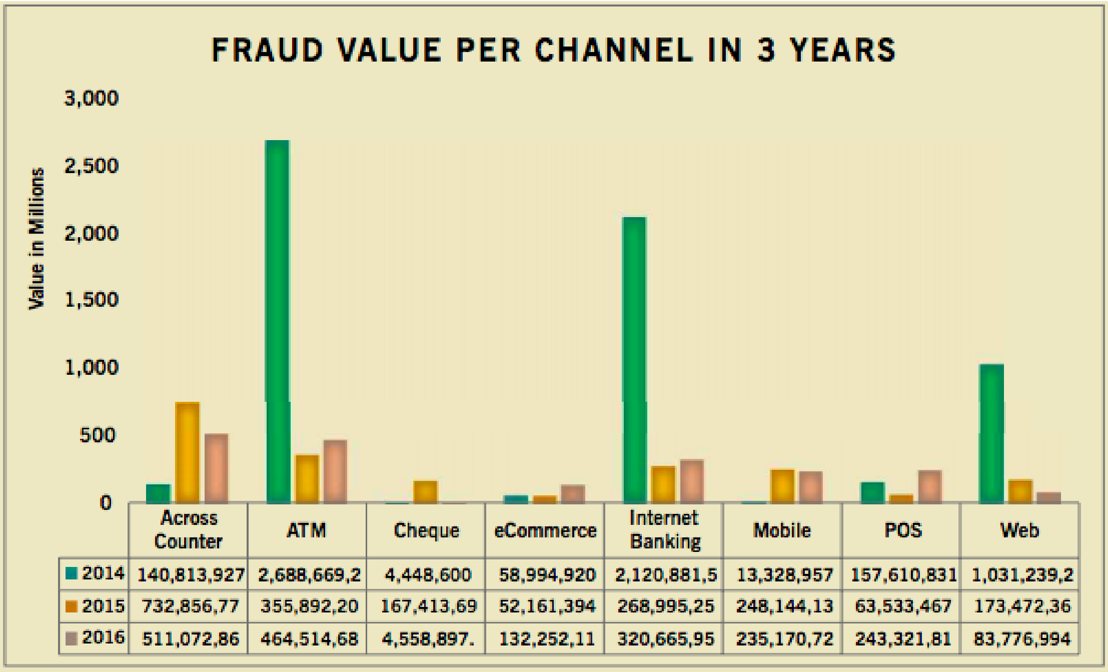
2.5.1 E-Banking Fraud in Nigeria

Nigeria has generally been slow to adopt e-banking services, and this may be attributed to the low level of confidence bank customers have due to the reputation of fraudsters and corruption in the country. There is a similar trend across Africa as 80% of adults in Sub-Saharan Africa still pay for their bills via cash transactions (Ogbalu, 2016). Intriguingly, although 77% of Nigeria's banking customers use social media, only 42% of them use online banking services (KPMG, 2017). Part of the reasoning for this may be due to the need for the banks to reinforce customer trust regarding the security of their e-banking services. In 2009, a survey of e-banking adoption found that although the users found e-banking useful and convenient, privacy and data security were the major issues affecting the perceived credibility of e-banking solutions at the time (Oni and Ayo, 2010). Ayo *et al.* (2007) also found that security was one of the major threats to e-banking adoption. Similar research has been carried out globally such as the work of Sravanthi (2016) and Makarevic (2015) whom both found that risks relating to security were common issues impacting e-banking adoption.

Although the overall adoption of e-banking has been slow, there has been a growing reliance on e-banking services as customers are becoming accustom to the benefits. In a 2014 customer survey, it was found that the ATM was the most important service measure for retail customers (KPMG, 2014). The same survey found that the ATM was by far the most popular channel amongst retail consumers in Nigeria with 80% of customers preferring to withdraw money at the ATM rather than at the bank branches. This increase in adoption may have been due to the benefits of e-banking services such as convenience, but may also be due to the improved security by the banks

Research by Idolor (2010) found that the CBN regulatory framework was effective in helping reduce fraud across the industry. However, although improvements have been made, e-banking fraud remains a challenge, both in Nigeria and globally. In 2011, CBN stated that fraud cases were perpetrated through means such as pilfering and theft, suppression and conversion of customer deposits, illegal funds transfer and fraudulent ATM withdrawals (CBN, 2011). By 2016, fraud continued to be a challenge with over the counter and ATM services identified as the areas where the biggest losses were made. This indicates that a large proportion of fraud in Nigeria is executed through e-banking mediums.

As the adoption of e-banking services in Nigeria grows, the number of fraud occurrences have also been on the increase. In 2016, there was a total of 19,532 fraud cases compared to 10,743 in the previous year (NeFF, 2017). This shows a significant increase in the number of fraud cases, nearly doubling in the space of a year. However, although there was an increase in the number of fraud cases, the actual financial losses were on the decline and had decreased compared to the previous year. The table below provides a view of fraud cases from 2014 to 2016.



	Across Counter	ATM	Cheque	eCommerce	Internet Banking	Mobile	POS	Web
🟩 2014	140,813,927	2,688,669,2	4,448,600	58,994,920	2,120,881,5	13,328,957	157,610,831	1,031,239,2
🟧 2015	732,856,77	355,892,20	167,413,69	52,161,394	268,995,25	248,144,13	63,533,467	173,472,36
▨ 2016	511,072,86	464,514,68	4,558,897.	132,252,11	320,665,95	235,170,72	243,321,81	83,776,994

Figure 2.2: Three Year Fraud Value Per Channel in Nigeria (NeFF, 2017)

The figure above depicts a consolidated view of fraud per channel across all banks in Nigeria. It highlights the continued drop in fraud per channel, evidencing that fraud values were significantly less than before. The figure also highlights the progress made on the primary e-banking channels that frauds have been historically carried out from such as ATMs and internet banking. For example, a comparison of these figures with the global card fraud trends reported earlier indicates that Nigeria has made progress in securing its e-banking mediums.

Although the fraud values per channel have been generally on the decrease, Pam and Ozoya (2016) investigated into fraud and crime prevention and concluded that there is low reporting of fraud cases by victims. This implies that the cases of fraud may be higher than the fraud statistics that are published. There has been other research in Nigeria to obtain insights from fraud data. For example, Adeniyi (2016) analysed fraud in Nigerian banks and concluded that the total number of fraud cases cannot be used to predict the total expected losses to the bank. Aransiola and Asindemade (2011) conducted research to understand the profile of the perpetrators and the strategies that they employ. It was found that most of the cybercrime perpetrators in Nigeria are between the age of 22 and 29 years, who were undergraduates.

Research in Nigeria has also been carried out to understand the causes of fraud. In 2011, it was found that Socio-Economic factors such as unemployment and poverty are both contributory factors to fraud (Igwe, 2011). More recently, Omodunbi *et al.* (2016) highlighted that unemployment, quest for wealth, lack of strong cybercrime laws and insufficient security on computers as the main causes. This emphasises the influence of socio-economic factors on fraud. Banking customers' vulnerability to fraud is another factor that has been studied to understand its impact on fraud. Choplin *et al.* (2011) conducted a psychological investigation and found that factors such as education and demographics both influenced consumers' vulnerability. Additional e-banking security related studies from Nigeria are also discussed further within this chapter.

2.5.2 E-Banking Fraud Types

The types of fraud that are commonly experienced by financial institutions include sales fraud, purchase fraud, cheque payment fraud and ATM fraud (Benjamin and Samson, 2011). E-banking services are targeted for fraud and cybercrime using a variety of methods. These are discussed below.

Identity Theft

Identity theft can be described as the unauthorised access to personal information or documents and can be used for financial or non-financial gains (Sproule *et al.*, 2007). Newman and McNally (2005) explains that identity theft related crimes take place in three phases:

1. Acquiring the identity of the victim
2. The identity theft action
3. The outcome of the identity theft

From an e-banking perspective, fraudsters steal or create a fake identity with the intention of carrying out fraudulent transactions. Identity theft usually leads to fraudsters using an account of an existing person, creating a new account for an existing person or creating an account of a synthetic person, which is more common (Schreft, 2007). All three scenarios can be carried out over e-banking mediums and therefore are of relevance. Pam and Ozoya (2016) explains that fraudulent transactions via online platforms are one of the ways which fraudsters may use stolen information to defraud people. Furthermore, statistics have shown that identity theft leading to fraud has been on the increase since then. An identity theft report states that 15% of consumers had been victims of identity fraud (Javelin, 2017). This highlights the extent of the threat identity theft possesses.

Identity theft can happen via outside attacks or insider attacks. Outside attacks are people from outside the organisation or environment who use techniques such as hacking and malware to unlawfully gain access to data. Worryingly, the sophistication and frequency of cyber-attacks against financial institutions are on the increase (Camillo, 2017). Therefore, outside attacks is a challenge which banks must continue to safeguard against.

Insider attacks take place by insiders who have access to identity related information and abuse their access to obtain information (Gercke, 2007). This is also a pressing issue for banks as it involves their own staff who usually have access to systems and data. This is further discussed below.

Internal Bank Fraud

It is easy to assume that fraud is carried out by outsiders, but that is not always the case because fraud also takes place internally by bank staff (Cummins *et al.*, 2006). Dagogo and Ngerebo (2018) highlighted three broad categories for the perpetrators of bank fraud; internal, external and mixed. Therefore, two of the categories involve internal bank staff. The bank staff are more capable of compromising security systems and controls to either carry out fraud themselves or aid others to carry out fraudulent transactions. Research by Aransiola and Asindemade (2011) also showed that internal personnel of banks had been collaborating with fraudsters. This presents a real threat as employees are more aware of the security measures being employed to protect against such activities, and therefore more likely to know where loopholes exist. It is understood that 25% of an organizations data breach cases involve internal actors (Verizon Enterprise, 2017). An investigation into the threat from insiders revealed that privilege abuse amounted to 88% of previous incidents (Verizon Enterprise, 2014). This provides a perspective on the extent of the challenge associated with employees within organisations.

Although research is limited to understand why staff carry out fraudulent activities for companies they are employed by, Benjamin and Samson (2011) investigated into the perceived inequality and perceived job insecurity on fraudulent intent of bank employees in Nigeria and found both factors to have a significant effect on employee fraudulent intent. The study also revealed that age has a significant effect on fraudulent intent. Banks should therefore take these under consideration and ensure they adequately mitigate these risks.

Phishing

Phishing involves the stealing of personal information from unsuspecting users (Omodunbi *et al.*, 2016). It is a mechanism that fraudsters use to obtain customers personal details leading to its use for fraud and has previously been touted as the most worrying development in the financial sector (Reavley, 2005). It is a type of social engineering which attempts to persuade potential victims by appealing to their emotions to create a feeling of trust (Gao and Kim, 2007). Fraudsters who are able to retrieve personal information such as PIN, passwords and data that can be used to apply for credit can sell this data online to anonymous brokers (Moore *et al*., 2009). The figure below depicts how phishing is used by fraudsters to steal data.

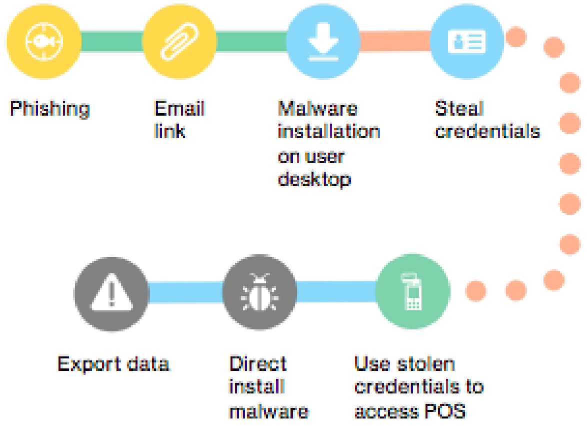

Phishing
Email link
Malware installation on user desktop
Steal credentials
Export data
Direct install malware
Use stolen credentials to access POS

Figure 2.3: Birth and Rebirth of a Data Breach (Verizon Enterprise, 2016)

Phishing emails are becoming more sophisticated and tend to include information such as company names or logos to build source credibility, and convince those that are targeted (Workman, 2008). Statistics show that 35.9% of the financial sector is the target for phishing. Therefore, it’s not only the customers that are being targeted. Vulnerabilities in online banking systems have been exposed by techniques such as cross-site scripting, click jacking, MIME sniffing and cross site request forgery (Sood and Enbody, 2011). These are all used to steal information from sessions indicating the importance of browser security. Although research is being constantly carried out to find ways of identifying, and mitigating the risk phishing, it still remains a pertinent challenge.

Card Skimming & Cloning

Card skimmers are essentially devices that are placed over card readers at ATMs or POS devices to retrieve information for fraudulent purposes (Daw, 2012). The fraudsters use this technique with increasingly sophisticated technology to steal customers card data without them even noticing. This information is then used to produce counterfeit cards which are difficult to differentiate from the genuine card (Budhram, 2014). In Nigeria, Pam and Ozoya (2016) also found that skimming techniques included pin cushions and cameras secretly installed by criminals to capture the customer’s PIN. Customers are therefore required to be vigilant when using card payment devices and ATMs. Magnetic strip cards are most vulnerable to card skimming. For example, the US relied hugely on magnetic strip cards and as a result, a survey found that 42% of Americans had experienced some form of payment card fraud over a 5-year interval (Economist, 2014). Such high figures indicate that magnetic strip cards represent a huge security challenge to bank customers.

After carrying out the activities to steal personal or financial information required to perform fraud. The next step is for fraudsters to actually carry out the fraudulent transactions, either remotely or physically.

The above section has therefore helped answer the first research question.

Research Question 1: What are the security challenges’ that banks experience while offering e-banking services?

Although fraud remains a menace, there has been some progress in preventing fraud with statistics showing a decrease in losses in recent times. Subsequently, there was a need to understand what factors have been critical in preventing fraud over electronic mediums and this is discussed later within this chapter. The next section highlights the theory which underpinned the study.

2.6 Theoretical Framework

This section proceeds to review existing theoretical frameworks which were considered for this research to allow a suitable theory to be adopted. Given that the research sets out to understand the most important factors and activities associated with preventing e-banking frauds, the following theories were considered:

- Cost/Benefit Analysis.

- Critical Success Factors
- Key Performance Indicators
- SWOT Framework
- Theory of Planned Behaviour

2.6.1 Cost/ Benefit Analysis

The Cost/Benefit Analysis is a means of weighing up the benefit of particular measures or solutions against its costs to be able to make an informed decision. It can be a highly detailed and important procedure for deciding whether resources should be allocated to a project or instead diverted for other uses (Boardman *et al.*, 1998). Nortman *et al.* (1986) described 'cost-benefit' where the cost of a service should not exceed its benefits. It has been argued that cost benefit analysis should be comprehensive and based on all factors relevant to the decision-making process, not solely based on economic arguments (Ewusi-Mensah, 1989). To address the challenge of subjective criteria applied by decision makers, Carlesi (1981) proposed that an objective method of cost/benefit analysis which also considers predefined criteria and intangible benefits is used.

The application of the Cost /Benefit theory would be more suited to research evaluating specific measures for preventing fraud. For example, if there was a focus on a specific fraud prevention technology, a cost/benefit analysis could be utilised to ensure the benefits outweigh the costs of adopting that technology.

2.6.2 Critical Success Factors (CSF)

Rockart (1979) defines CSF as the limited number of areas in which results, if they are satisfactory, will ensure successful competitive performance for the organisation. Similarly, Shank *et al.* (1985) defined CSF as the few things that must go well to ensure success. CSF are imperative in concept yet highly practical and as such readily understood and accepted by managers and practitioners (Butler and Fitzgerald, 1999). This may be one of the reasons why the CSF theory is becoming more widely adopted for research. CSF represent managerial or individual activities that an organisation must pay attention to achieve the desired goals Hackney & Dunn (2000) cited in (Sebora *et al.*, 2009). This theory has been utilised for a variety of studies ranging from manufacturing to IT system implementations. Rockart (1979) adopted CSF theory for corporate strategic planning, to highlight the key information requirements of top management.

The CSF theory has been utilised for many information, business and technology planning methodologies (Caralli *et al.*, 2004). It has been adopted in the context of security such as the studies by Bobbert and Mulder (2015) on business information security and Humphrey (2017) on CSF for incident reporting. CSF theory has also been used in the context of banking such as e-banking adoption by Shah and Siddiqui (2006) and branchless banking (Kumar and Gupta, 2009). Previous research adopting the CSF theory has resulted in the identification of factors through a wide array of approaches using quantitative and qualitative research methods (Esteves and Pastor, 2004).

In strategic management, a similar concept referred to as Key Success Factors (KSF) are used. According to Grunert and Ellegaard (1992), KSF have been used in four ways; as an ingredient in a management information system, a unique characteristic of a company, a tool for managers to sharpen their thinking, and as a description of the major skills and resources required for successful performance. In contrast, Critical Failure Factors (CFF) is a different approach that can be used to identify factors that tend to cause failure. Research shows that this approach is used less often and is suited to scenarios where frequent failures have occurred leading to the need to identify such factors and classify them, to help prevent failures in the future (Amid *et al.*, 2012). However, Aziz and Salleh (2011) contradict this by arguing that identifying the CSF has become the main agenda for researchers due to the wide numbers of failures reported, implying that the application of the CSF theory can be applicable in both contexts.

2.6.3 Key Performance Indicators (KPIs)

Since raw data can be difficult to interpret and can be meaningless, businesses started calculating KPIs. They are usually measures critical to an organization’s core business (Seang, 2003). Research related to KPIs is specific to industries or measure functional performance for particular situation, there is no unified approach to define KPIs (Skibniewski and Ghosh, 2009). The key characteristics of KPIs as defined by Feldman (2011) are captured below:

1. Non-financial measures
2. Measured frequently
3. Acted on by the senior management team
4. Measures that time responsibility down to a team
5. Have a significant impact
6. Encourage appropriate action

In addition to the characteristics above, KPIs should be comparative and directional whilst also addressing lagging and leading indicators (Simon, 2015). In terms of KPI definition, it is recommended that the relevant stakeholders start with the basics to understand the objectives of adopting the KPIs whilst also going through an iterative process with regular feedback from management (Sari, 2015). The approach for implementing the Key Performance Indicators should be based on three concepts (Shah and Siddiqui, 2006):

1. Determination of a set of key indicators concerning the general health of business. Information is collected on each of these indicators.
2. Exception reporting regarding the availability of information to executives on areas where organisational performance is different from predetermined criteria.
3. Increasing the availability of better, cheaper and more flexible visual display techniques to help executives to digest vast quantities of information.

Indicators have been used in previous studies related to bank fraud such as the work of McAteer (2009) where performance indicators for management fraud were used as a tool for detection of management fraud. KPIs have also been used for financial institutions information security governance. Research was done to calculate the KPIs for financial institutions by conducting a survey to review the institutions assignment and supervision responsibilities, security organization, security practices and security investment management (Kryukov and Strauss, 2009). Similarly, KPIs have also been used as a tool for evaluating security controls (Abercrombie *et al.*, 2008).

KPIs do present some challenges for organisations to overcome. Firstly, there is a reliance on the availability of data to be able to calculate defined KPIs. Secondly, organisations must know which areas they wish to monitor performance on. As this research focussed on understanding the most effective factors for e-banking frauds prevention, defining KPIs was not suitable for meeting the research objectives. However, KPIs can be used to measure the performance of measures identified by CSF and further details is covered later within this chapter.

2.6.4 SWOT Framework

SWOT stands for Strengths, Weaknesses, Opportunities & Threats, and is used for analysis to provide a systematic approach to support strategic decision making (Menga *et al.*, 2015). SWOT can be performed by the individual managers or in groups. Group techniques are particularly effective in providing structure, objectivity, clarity and focus to discussions about strategy which might otherwise be influenced by politics and personalities (Glass and Schmidt, 1991). The SWOT framework has also been involved in hybrid decision making methods such as the work of Kurttila *et al.* (2000) where the SWOT analysis was combined with the Analytic Hierarchy Process, a commonly used method for decision analysis.

The SWOT framework has been applied in a broad range of scenarios in the banking industry. Nyandoro and Mahleko (2015) used the SWOT framework to analyse mobile banking services in Zimbabwe. In Nigeria, the SWOT analysis was used to analyse the prospects of mobile commerce (Ayo *et al.*, 2007). The SWOT framework was applied to the Lloyds Banking Group, and the analysis was for the bank entirely rather than focussing on a particular service or technology (MarketLine, 2012). Therefore, it can be used for either broad or narrow contexts. The SWOT approach has also been used to identify areas where research, standardization and development is required for mobile privacy and security (Hulsebosch *et al.*, 2004). This particular scenario indicates that there could be a particular focus on one or two of the areas, such as weaknesses or opportunities. This also aligns with the work from Yasar *et al.* (2012) where research was carried out to identify the advantages of using cyber electronic warfare. Although the focus of the research related to area of strengths, the SWOT analysis was still adopted for use.

The SWOT analysis is now one of the most frequently employed instruments in strategic analysis, but also in other evaluative studies (Al-Araki, 2013). For the purposes of this research, the SWOT framework was not the most suitable because it does not go into the details of how or why for each of the areas defined as the strengths, weaknesses opportunities and threats. Such a framework would add more value if the research concentrated on a particular fraud prevention measure or technology. There has also been previous research where the SWOT analysis was used as a decision-making aid for selecting appropriate frameworks (Mishra and Chakraborty, 2014). Similarly, the SWOT analysis was used on a security framework to protect against cyber-attacks (Trim and Yang-Im Lee, 2010). Therefore, there is an opportunity to use the SWOT analysis for future work once the framework has been defined.

2.6.5 Theory of Planned Behaviour (TPB)

An alternative theory would be to adopt the Theory of Planned Behaviour (TPB) which is a behavioural decision-making model. The concept initiated from research that examined the relationships between attitudes and behaviours (Armitage and Conner, 2001). This theory can be applied to various types of behaviours based on their beliefs and can be used to understand the actions or activities that can influence the likelihood of the behaviours happening. Attitude, subjective norms and perceived behavioural control are the 3 factors that TPB proposes that intension is influenced by.

Research using this theory in the context of electronic security exists. For instance, Safa and Von Solms (2016) used the TPB to consider the impact of knowledge sharing in organizations. Archer (2011) adopted the theory to identify behaviours associated with identity fraud detection.

The challenge associated with this approach is the reliance on self-reporting, thereby subjecting the data to bias (Armitage and Conner, 2001). In addition, because this study focusses on prevention, the data will need to be obtained from either fraud victims or people who have been involved in carrying out fraud. The confidential nature of this may restrict the ability to collate data. The researcher decided that this theory was not best suited to meet the objectives of this.

2.7 Theory Adopted for the Study - CSF

After consideration of theories for the purposes of this study, it was decided that the Critical Success Factor (CSF) theory was the most appropriate. More importantly, further review confirmed that the CSF theory would enable the research aims and objectives to be met. Evidently, studies have shown that the use of CSF can help achieve high performance through a variety of areas such as for strategic planning, implementing plans or establishing guidelines for organisational activities (Boynton and Zmud, 1984). Caralli *et al.*, (2004, p.11) stated that strategic CSF “are more than just guiding principles; instead, they are considered to be an important component of a strategic plan that must be achieved”.

One of the deciding factors for selecting the CSF theory is its ability to derive into additional details for factors rather than solely for the identification of factors. In addition to identifying CSF, the theory helps derive other useful information to support information systems strategic planning (Amberg *et al.*, 2005). For example, the theory allows for weighting and ranking of factors, analysis of relationships, and key activities for each of the factors to be identified. The adoption of the CSF theory also provided an opportunity to amplify the key aspects from different perspectives such as people, processes and technology.

There is no theory that is faultless. Previous research has surfaced some of the weaknesses of the CSF theory. Imroz (2009) mentions that CSF can be subjective as the identification process usually involves interacting with relevant people on the topic, leaving room for bias based on their experience and concerns appropriate to their position. The study recommends that participants in studies should include a wide spectrum of positions. This aligns with the recommendation by Bullen and Rockart (1981), as they suggested that managers from multiple levels of an organisation’s hierarchy should be interviewed. To further strengthen the argument, Boynton and Zmud (1984) also found that CSF may leave room for bias and suggested that they should be identified by a combination of managers and analysts. However, the study still found that CSF were particularly effective for supporting planning processes. The common theme from previous research is that a variety of relevant participants should be engaged in the CSF identification process.

The adoption of this theory also paves way for some of the alternative theories that were considered such as the SWOT analysis and KPIs to be used for future work. The CSF theory has been already used in e-banking and security related studies, but not in the context of this research. The table below summarises previous research and methodologies that were adopted.

Table 2.1: Summary of Previous CSF research relating to E-Banking & Security

Research Topic	**Reference**	**Methodology**
Identifying the critical success factors to improve information security incident reporting	Humphrey (2017)	- Delphi Method
Governance practices and critical success factors suitable for business information security	Bobbert and Mulder (2015)	- Literature Review - Focus Groups
Information Security Culture	Alnatheer (2015)	- Literature Review
Critical Success Factors for The Implementation of a Security Policy in Health Clinics	Lopes and Oliveira (2015)	- Survey
Conceptualizing and Examining the Critical Success Factors for Implementing Islamic Banking System Towards Banking Sector of Iran: A Mixed Method Approach	Javadin *et al.* (2015)	- Literature Review - Interview - Survey
Critical Success Factors Analysis on Effective Information Security Management: A Literature Review	Tu and Yuan (2014)	- Literature Review
From Information Systems To E-Learning 3.0 Systems' Critical Success Factors: A Framework Proposal	Miranda *et al.* (2014)	- Literature Review

Improving Organisational Information Security Management: The Impact of Training and Awareness	Waly *et al.* (2012)	- Survey
Critical Success Factors for An Effective Security Risk Management Program: An Exploratory Case Study at a Fortune 500 Firm	Zafar *et al.* (2011)	- Case Study
Application Of Q-Methodology in Critical Success Factors of Information Security Risk Management	Imroz (2009)	- Interviews
Branchless Banking & Financial Inclusion	Kumar and Gupta (2009)	- Survey
A Change Strategy for Organisational Security the Role of Critical Success Factors	Foster *et al.* (2007)	- Literature Review
Managing Information Systems Security: Critical Success Factors and Indicators to Measure Effectiveness	Torres *et al.* (2006)	- Literature Review
Organizational Factors to The Effectiveness of Implementing Information Security Management	Ernest Chang and Ho (2006)	- Literature Review - Survey
Critical Success Factors For E-Banking Adoption	Shah and Siddiqui (2006)	- Literature Review - Case Study
Establishing A Foundation for Enterprise Security Management	Caralli *et al.* (2004)	- Case Study - Survey

The table above summarises the previous CSF studies which have been carried out. Of those that are security related, none identify CSF for frauds prevention in the context of e-banking, a gap which this study set out to fulfil.

2.7.1 CSF Theoretical Framework

Paramount to establishing the research design was the development of the theoretical framework underpinning the research. Having reviewed literature relating to the CSF theory, the following conceptual framework was proposed. Given that the primary aim of the study was to identify CSF for EBFP, the framework outlines the approach to achieve this. The research methodology which is described in the next chapter describes the research methods that were adopted to apply this framework.

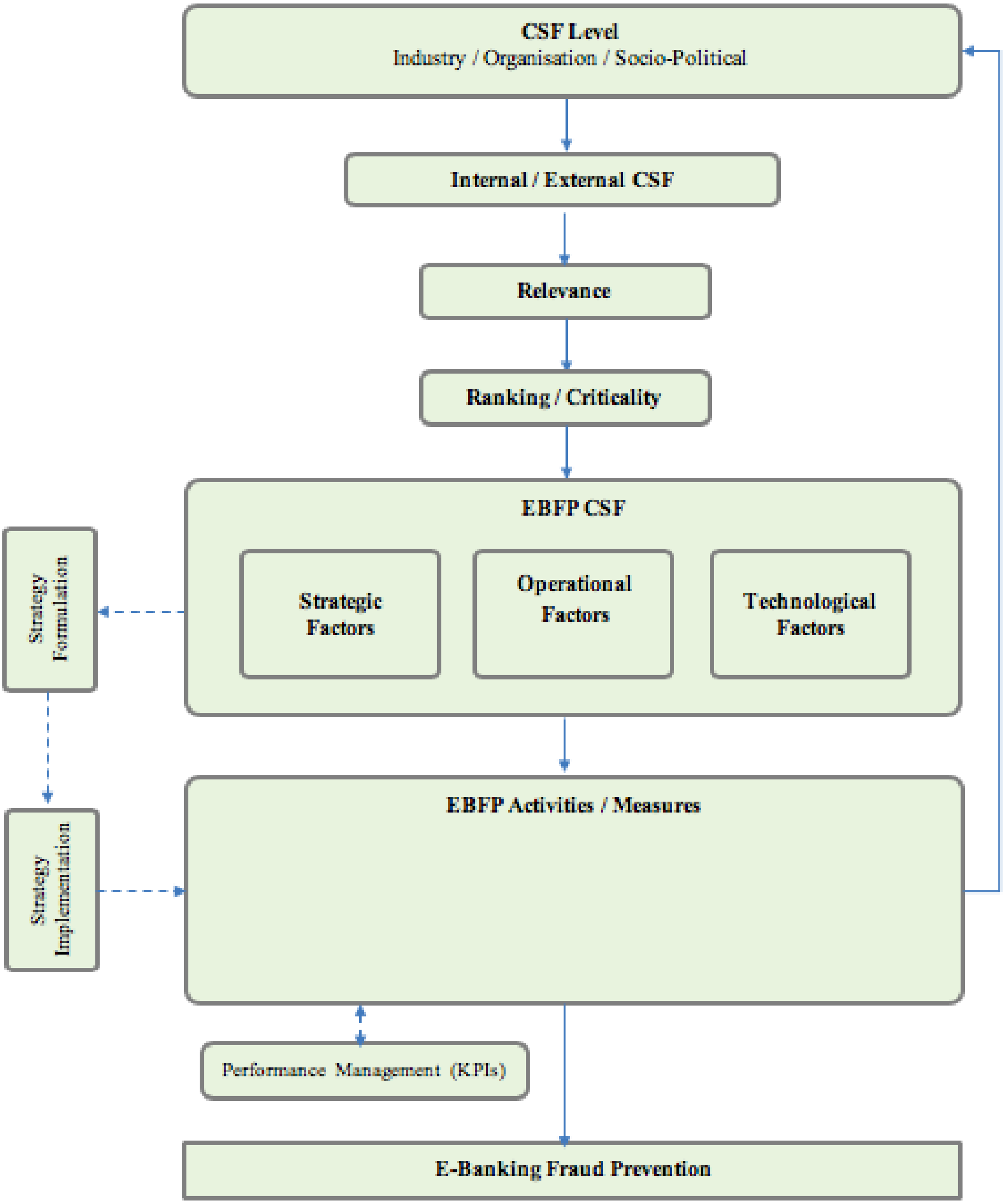


Figure 2.4: Theoretical Framework for the Identification and Application of CSF

Figure 2.4 depicts a summary of the theory relating to the identification and application of CSF. The subsequent sections provide an insight into each of the areas covered in the theoretical framework, referring to existing theory and studies.

2.7.2 CSF Levels

Leidecker and Bruno (1984) states that there are 3 CSF levels. These are industry, firm specific, and economic socio-political environment. The industry level focuses on analysing certain factors in the basic structure of an industry that would help significantly improve the company’s performance across that industry. The firm specific CSF focuses on specific organisations within internal focus. Whereas the economic socio-political level goes beyond the industry to scan the environment for sources which can help and identify these CSF. Leidecker and Bruno (1984) argues that all three of the levels are credible sources for identifying CSF. Other researchers such as Shank *et al.* (1985) also recommend the need to consider the socio-economic environment. On the contrary, rather than including it as a separate level, it is considered as external factors for the other levels. In addition, Bullen and Rockart (1981) introduced another two levels of CSF claiming that even within organisations CSF can be identified for business units as well as individuals. This therefore demonstrates how the CSF theory can be employed to cater to a broad spectrum of levels.

The primary focus of this research was to identify the CSF at the organisational level to help banks and financial organizations adopt and prioritise key factors used to address threats of fraud. Organisational CSF are used to identify CSF common to companies operating within the similar environments, in this case those that offer e-banking services. The banks can then use this information to define the CSF for other layers under the hierarchy such as specific business units and managers based on their organisational structure and priorities. Additionally, research from Tarafdar and Vaidya (2006) suggests that organisational factors can lead to the improvement of security management providing further justification for the CSF to be identified at this level for this research.

2.7.3 Internal and External CSF

CSF can be either internal or external in dimension. Internal CSF have related actions that can be taken within an organization while external CSF relate to actions that are taken outside of the organization (Flynn and Arce, 1997). Rockart (1979) stressed the need to identify which of the dimensions would be covered to ensure there is a focus on collecting information from the right sources. This study primarily focused on internal CSF relating to actions that banks can take internally to help minimise fraud over e-banking mediums. External factors such as economic and political environment in which may affect EBFP were omitted from this study given that organisations have limited control over such factors.

Khandelwal and Ferguson (1999) argue that all CSF can be defined as temporal or as ongoing CSF. Therefore, CSF which are either internal or external in dimension may be continuous or temporary. Although ongoing CSF are more common in literature, temporal CSF are usually associated with project related CSF where a factor might be temporarily critical for one or a few project phases.

2.7.4 Relevance of CSF

The relevance and criticality of CSF work hand in hand. Generally, as CSF are seen to be the most important factors, it is assumed that the factors will be of relevance if the right identification technique has been followed. However, some researchers chose to specifically study the relevance of CSF by using methods such as surveys and case studies. Typically, participants are asked to rank the CSF in terms of their relevance. Somers and Nelson (2001) or Pinto and Slevin (1988) are examples of popular CSF studies that involved participants ranking CSF with respect to their relevance.

To ensure relevance of the CSF identified, an iterative process during the literature review was adopted whereby the factors were only deemed relevant where they were recurring in literature and in similar contexts. Additionally, subsequent phases of the study provided opportunities for professionals in the banking industry to validate the factors, further ensuring relevance to the topic.

2.7.5 CSF Criticality and Validity

Boynton and Zmud (1984) suggested that managers should be involved in weighting CSF to help ensure reliability. This has been reflected in CSF studies such as research by Dwyer *et al.* (2000) where targeted survey respondents were asked to rate how critical CSF were using a Likert scale. Historically, the criticality of CSF has been assumed to be static. Pinto and Slevin (1988) argued that this is not the case as a study into examining the changes in CSF criticality over a project lifecycle found that the criticality does change over the lifecycle of a project. Although this relates specifically to project environments, they did also argue that CSF may be contingent to other phenomena such as organizational lifecycle. This therefore suggests that although there are benefits of rating CSF criticality, there is a need for the CSF to be periodically evaluated by organizations.

Ranking or rating criticality is a means of validating CSF. The validity of the CSF approach has been previously questioned due to the potential bias than can be introduced during interviews from managers and other staff. However, Boynton and Zmud (1984) indicated that there have been studies to prove that these biases can be overcome. Given that potential bias is a major challenge when identifying CSF, validation has become common activity for CSF research. Validation provides an opportunity to examine the conceptualisations and assumptions underlying the problem situation that is to be influenced (Fischer, 2003). Previous studies have taken one of the three approaches to validate CSF:

1. Validation of CSF through multiple sources within a single research method. An example of this is where an interview research method has been adopted and feedback from various interviewees have been analysed to validate a CSF. Alternatively, in case studies, an analysis within a case or cross-case analysis can be used to validate CSF.
2. Validation of CSF across multiple research methods.
3. Validation of CSF via a combination of approach 1 and 2 mentioned above.

Imroz (2009) provides an example of the second approach which involved a literature review to identify CSF followed by an interview of 50 IT professionals to validate them. It does also appear to be common for validation to extend across multiple research methods because at times additional factors are introduced at later stages of the research which also require validation. Zafar *et al.* (2011) provides an example of this where an interview after an initial survey revealed new factors that needed to be validated in the final phase of the research. Therefore, depending on the nature of the research design, there may be need for multiple instances of validation.

2.7.6 Techniques for Identifying CSF

Leidecker and Bruno (1984) recommends that internal staff of organizations are involved in the identification of CSF. Similarly, the process should ensure that the people involved have a fair knowledge of the industry (Barat, 1992). The range of methods adopted for CSF studies has been outlined in Table 2.1 above and can be summarised below.

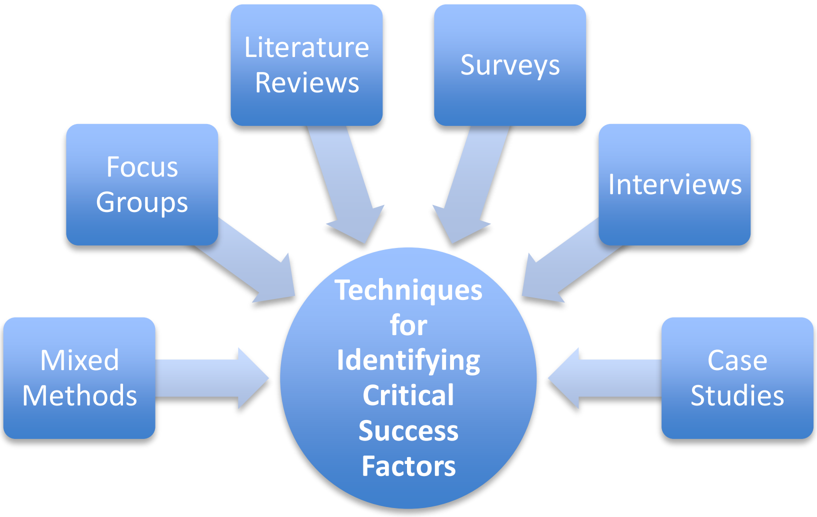


Figure 2.5: Techniques for Identifying CSF

Khandelwal and Ferguson (1999) summarises the different research methods along with their strengths and weaknesses. A common theme from previous studies is that the identification of CSF involves drawing from peoples experience and expertise. Barat (1992) emphasised that CSF are events and conditions in a few areas that are required for the business to succeed. Therefore, the expectation is that the factors will not be large in number, but rather specific and concise conditions that the banks must meet to be able to prevent fraud. It has been suggested that a group of over 12 factors is too large to be meaningfully considered (Barat, 1992). In contrast, Javadin *et al.* (2015) suggests that CSF should be measurable and a few in number. A review of previous CSF studies highlighted that CSF ranged from 5 to 10 in number. In security related research, Zafar *et al.* (2011) identified 9 CSF for effective security risk management, Alnatheer (2015) identified 8 CSF for Information Security Culture, Shah *et al*. (2007) and Yaghoubi et al. (2016) both identified 6 CSF for e-banking related studies. Such information helped provide guidance in terms of assuring that the quantity of CSF identified were comparable to previous research where the CSF theory had been adopted.

2.7.7 CSF Categories

CSF are commonly characterised in studies to help organise the factors. Organisations usually adopt a mixture of strategic and tactical factors to ensure short, medium and long-term planning can be catered to (Ward, 1990). The following CSF categories have been widely adopted in literature to differentiate CSF and was also adopted for this study:

- Strategic Factors: This identifies strategic issues and measures that the banks should implement or offer. Strategic factors require long term planning and can be uncertain or risky in nature. They identify issues that require close management attention (Boynton and Zmud, 1984)
- Operational Factors: This identifies the specific operational issues in governance or processes which need to be carried out. This is one of the most common categories of CSF and evident in previous CSF literature. Bai and Sarkis (2013) and research by Caralli *et al.* (2004) for operational factors relating to enterprise security are both examples of this.
- Technological Factors: This covers the factors relating to technology. These CSF are common in research relating to electronic services. Shah *et al.* (2007) identified technological CSF in a study relating to e-banking adoption whilst Selim (2007) found that some of the crucial CSF were technological whilst investigating CSF for e-learning. Miranda *et al.* (2014) identified technological factors whilst utilising the CSF theory to propose a framework.

2.7.8 CSF Sub-Factors & Activities

It is suggested that target activities should be used to enable organisations to realise the CSF (Bullen and Rockart, 1981). CSF tend to have activities or measures that relate to them, providing actionable insights on how that factor can be met. In effect, they provide further guidance on how a CSF can be achieved. Literature has shown that CSF can have various layers consisting of factors, sub-factors and activities. Although some studies identified factors only, others provided further details such as factor categorisation, sub-factors and activities for the factors.

Most of the literature reviewed found that CSF research at minimum was similar to that of Ho and Lin (2004) which identified CSF, arranged them into categories and provided descriptions of the factors. Several studies aligned with this (Dwyer *et al.*, 2000; Jalonen and Lönnqvist, 2011; Alnatheer, 2015). Caralli *et al.* (2004, p.65) adopted a similar approach as the CSF identification process resulted in CSF which were then broken down into “supporting themes” and “activity statements”. The study explains that supporting themes provide a description or definition of the CSF whilst the activity statements reference activities that an organisation may already be doing or should be doing. Therefore, offering further insight on the activities that can be carried out to achieve the CSF. In contrast, Ngai *et al.* (2008) identified sub-factors for some of the CSF. These were used in the cases where there are factors that are interrelated and can be summarised by a main factor. Similarly, Imroz (2009) used a factor analysis approach to condense the factors systematically into smaller groups. This study adopted a similar approach and the hierarchy is summarised in figure 2.6 below:

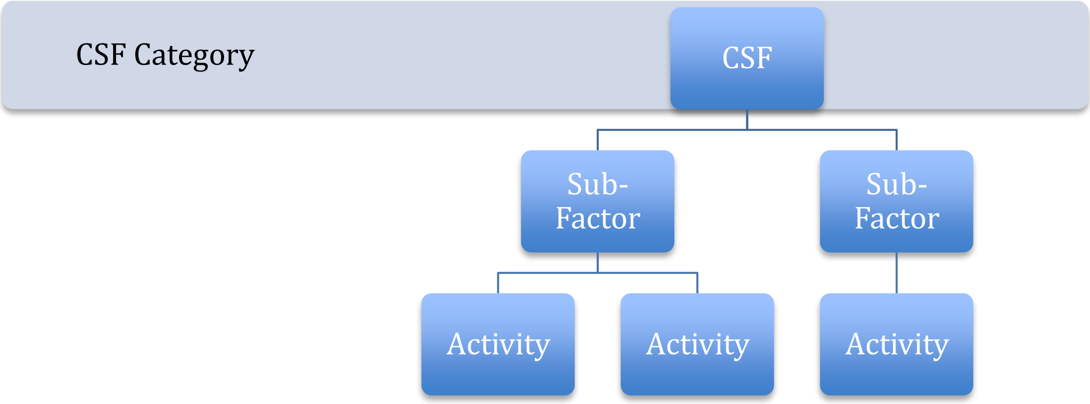


Figure 2.6: CSF Hierarchy (Sub-Factors & Activities)

Each of the CSF were aligned to a category as discussed in the previous section. Additionally, interrelated sub-factors for each of the CSF are given. Activities lie at the bottom of the hierarchy providing details on activities or measures that can be taken to help achieve the CSF.

2.7.9 Application of CSF to EBFP

As previously explained, CSF should be used for banks strategic planning and form input into their strategy. This is then cascaded down across the business and adhered to by incorporating them into their business processes. Ward (1990) explains that one CSF can require many business processes. After identifying CSF, banks should map their business processes to the CSF using a matrix to ensure each CSF has been adequately addressed (Van Veen-Dirks and Wijn, 2002). This approach helps evaluate whether there are sufficient processes to cater for the CSF requirements. Additionally, once CSF have been addressed, there should be a process in place to monitor performance.

2.7.9.1 Key Performance Indicators

Key Performance Indicators can be used as a tool to monitor the performance of CSF and was discussed earlier within this chapter as a theory that was considered to meet the objective of this study. Although it was not adopted for this study, literature suggests that KPIs can play an important role in achieving CSF. Caralli *et al.* (2004) suggests that any activities and initiatives organisations undertake should be to ensure high performance for the CSF. To monitor this, Baker (1995) suggests that introducing sustainable KPIs that cover all CSF and have the capability to provide useful information for areas of improvement. He also points out that there is no perfect number of KPIs that should be used. Therefore, Key Performance Indicators should be defined and monitored as a means of achieving high performance for the CSF.

2.7.9.2 Evolution of CSF

It is important to note that CSF are not definitive and can change over time. A change in context or in understanding from the participants' who contributed towards the identification of the CSF can cause the CSF to evolve (Williams and Ramaprasad, 1996). Similarly changes in environment or stage of firm development are examples of other causes for variance of CSF (Goldstein and Rockart, 1984). Notwithstanding, the researcher believes that the benefits which have been outlined earlier still outweigh these limitations.

Although researchers have surfaced this in different topics whilst discussing CSF relevance, a common argument is that CSF are not static and do need to be re-evaluated. Boynton and Zmud (1984) explained that CSF can be continually reviewed and revised to reflect the important issues in a dynamic environment. Williams and Ramaprasad (1996) also suggested a similar approach as it allows factors identified to be adequate and operationally feasible. Therefore, theory suggests that a constant review of the factors and their criticality is desirable to help maximise CSF benefits.

2.8 CSF for Preventing E-Banking Frauds in Banks

The following section outlines the findings from the literature review which identified a number of effective fraud prevention factors. As much as possible, constructs provided by previous studies have been used and the factors arranged into strategic, operational and technological factors to categorise the factors as done in previous CSF research.

2.8.1 Strategic Factors

Reporting – Timely Access to Information

Fraud reporting is regularly used to ascertain the performance of security systems. As such, it has been argued that KPIs used for electronic security should be included in financial intuitions KPIs (Kryukov and Strauss, 2009). This emphasises the important role that statistics have in monitoring fraud rates, understanding the impact of fraud prevention measures and aiding the decision-making process for both regulators and bank. For example, Igwe (2011) makes use of statistics to argue that advanced fee fraud is an issue not only in Nigeria, but also in many other countries. Without access to statistics and reports, it would be difficult to justify such a statement. Mechanisms for financial institutions to report suspicious activities to the relevant regulator and law enforcement agencies have also been identified as important (Federal Financial Institutions Examination, 2005). This allows law enforcement to quickly act and deter those who consider fraud. Therefore, timely access to information enables both banks and regulators to quickly respond.

Awareness of the Socio-Economic Climate

Social and community factors are equally important influencers on the perpetration and prevention of crime (Chua *et al.*, 2007). Similarly, Alfawaz et al. (2010) identified the social environment as an important security factor amongst other factors such as technology and regulation. Pulz *et al*. (2017) found that there is a correlation between socio-economic indices and fraud losses and called for the use of such indicators to predict fraud. A study from Igwe, (2011) found that socio-economic factors such as unemployment and poverty are both contributory factors to fraud. Given the above examples, it is necessary to consider the socio-economic environment. Although such factors are outside the control of the banks, being aware of the environment allows them to adequately adjust their prevention strategy. For example, banks may need to adapt their monitoring or controls based on poverty or fraud indicators.

Consumer Education

Banking customers vulnerability to fraud is an area that has been discussed severally. Choplin *et al*. (2011) conducted a psychological investigation and found that factors such as education and demographics both effect consumers' vulnerability. This ties closely with the work of Rizzardi (2008) where emphasis was placed on educating people on how to protect their personal information to prevent payment card fraud. Likewise, Roberds (1998) reaffirms this by highlighting privacy as a factor that affects the risk of fraud. Barker *et al.* (2008) explained the importance of including merchants in awareness trainings due to their role in accepting and processing payments.

There are numerous literatures advocating for the education of customers to prevent breaches of security. According to Puhakainen and Siponen (2010), training is one of the most commonly suggested approaches for information security policy compliance. Alnatheer (2015) conducted a study to identify the critical success factors for information security culture and found security awareness to be one of the top factors. This only further strengthened the findings from a study by Akpan (2013) where intensifying customer education was highlighted as one of the solutions for preventing bank fraud.

Cone *et al.* (2007) recommended that education trainings should be tailored to address the requirements of an organization. Therefore, banks may need to define a suitable curriculum to ensure that the training content includes all necessary information for increased consumer awareness of fraud, the current challenges and clear preventative steps that can be taken. Additionally, Javelin (2017) recommends that customers should be made aware of the importance of reporting incidents as soon as they occur to give banks and card issues the opportunity to prevent further fraud. Finally, it is recommended that information security training adopts content and methods that activate and motivate the learners to keep them engaged (Puhakainen and Siponen, 2010). This is to help the learners better absorb the content which is being taught to them.

Organisational Learning

Torres *et al.*, (2006) suggested that information security has become challenging to manage and near impossible to predict. His study explains that organisations are dynamically evaluating indicators such as incidents stopped and response times to learn and improve. Also, organizational learning requires organisations to learn from their own mistakes and other organizations' mistakes. Research relating to this argument exists as Roberds (1998) exposed that ignoring factors from historical lessons learnt had led to a costly fraud occurrence in retail payment. An example was given which a store’s value card could be beaten by cloning, which resulted in losses of at least $600 million. This is one of many examples where security lapses or weaknesses have resulted in large amounts of losses, but it appears that banks and other financial institutions have since learnt from it.

Shah (2016) suggests that organisations should systematically evaluate the effectiveness of identity theft prevention measures, enabling them to determine how well the controls in place are able to address the risks. Seltzer (2008) recommends that banks report statistics on identity theft attempts, the number of those that are successful, the form of theft and the type of banking product or service compromised. This will enable banks to assess how well their current security measures are performing and identify specific products or services that may be more exposed than others so that they can address the issues sooner rather than later. Safa and Von Solms (2016) considered knowledge sharing in organizations and found that information security knowledge sharing decreased the risk of security incidents.

Use of Specialist Third Parties

Another security measure involves employing the use of agencies that become intermediaries between the customer and banks. Such scenarios help support confidentiality, integrity, and authentication interactions Tan *et al.* (2002) as transactions are not directly linked to the banks systems. Opinions do vary in respect to what intermediaries should control but it seems that there could be both advantages and disadvantages to using them. Third parties have also been used to conduct objective gap analysis as highlighting vulnerabilities within organisations, which can be quite sensitive (Williams, 2014). It has been suggested that third parties can strengthen the customer authentication process by matching information to third part data sources or authenticate the individual on the bank’s behalf (FFIEC, 2005). These are some of the alternative uses of third parties to support organisations strengthen their security systems and prevent fraud.

Engaging Consultants / Specialists

The use of consultants can be used to strengthen e-banking security (Popo-ola and Olowookere, 2008). Consultants or specialists can be engaged in various stages for e-banking security ranging from recommending solutions to implementing them. There is need to engage consultants or specialists for securing e-banking systems (Foon and Fah, 2011). Banks use external consultants to develop or improve their customers online banking security (Abubakre et al., 2010). Some of the recommendations involve specialists for contingency and disaster recovery planning (Jin and Fei-Cheng, 2005). This provides some examples how consultants can be used in a variety of ways to support banks in preventing e-banking frauds.

Adaptive Policies, Procedures & Controls

Security policies should aim to protect people's data, systems and the organisations reputation. Adewale *et al.* (2014) identified having good adaptation of security policies and procedures as key to securing transactions, emphasising the need for banks to be dynamic in securing their electronic channels. It is recommended that banks also learn from historical risks and issues so that they can protect against them (Torres *et al.*, 2006). Hence, risk management can play a key role in preventing fraud, in the context of preventing banks against security risks which may lead to fraud but also for assessing the risk of transactions which is covered within the next section.

It is recommended that security policies include policies for IT risk assessment, penetration testing, vulnerability assessments, security awareness, incident management and IT audits amongst others (Streff, 2009). Beyond having a security policy defined, it is suggested that the key to controlling operational risks for e-banking lies in having effective policies, procedures and controls Khan and Karim (1997), cited in (Abdou *et al.*, 2014). The dynamic nature of e-banking and security therefore means that there is need for adaptive policies, procedures and controls.

Use of Historical Data to Predict Fraud

Security breaches are usually followed with the renewed call for the implementation of fraud prevention solutions (Crosman, 2017). For fraud to be successfully prevented and kept to a minimum, there needs to be a means for using historical data to predict and prevent fraud. It has been suggested that this can be achieved by using specialised data mining software (Songini, 2004). Efiong *et al.* (2016) also calls for the use of data mining, highlighting it as one of the most effective mechanisms for preventing fraud. Software can be used to, identify, block or reroute suspicions transactions. An approach for banks has been studied which detects behaviour and assign risk ratings for transactions so that fraud can be detected (Wei *et al.*, 2013). The transactions are monitored using various algorithms and makes a comparison with identified fraud patterns. A similar concept has been developed for the World Bank which involved using historical data to assign risk scores for their contracts to successfully predict instances of fraud (Grace *et al.*, 2016).

Banks that have implemented fraud prevention solutions have experienced a very quick return on investment (Lamont, 2010). Transaction monitoring using approaches such as artificial intelligence or transaction history was identified as the most effective model for preventing e-banking fraud (Abu-Shanab and Matalqa, 2015). Bank of the West, a bank in the US reported a significant decrease in fraud occurrences after implementing a fraud prevention tool which allowed them to achieve an accurate view of customer behaviour (Browdie, 2012). Recent figures have revealed that 67% of attempted fraud are now being stopped and this was attributed to strengthened security systems and consumer awareness (Financial Times, 2017). This highlights the impact that advancing systems are beginning to have.

Table 2.2: Summary of Strategic Factors for E-Banking Fraud Prevention

No	**Factor**	**Reference**
1	Timely access to information to empower management decision making	Federal Financial Institutions Examination (2005); Sidden and Simmons (2005); Kryukov and Strauss (2009); Koskosas (2011); Shah (2012)
2	Mitigation of consumer vulnerability to fraud by providing adequate Consumer Education	Hinson (2003); AbuZineh (2006); Torres *et al.* (2006); Barker *et al.* (2008); Mahdi *et al.* (2010); Puhakainen and Siponen (2010); Choplin *et al.* (2011); Akpan (2013);

		Alnatheer (2015); Javelin (2017); Krishnan (2017)
3	Awareness of Socio-Economic climate	Chua *et al.* (2007); Alfawaz *et al.* (2010); Igwe (2011); Pulz *et al.* (2017)
4	Engaging Consultants/Specialists	Jin and Fei-Cheng (2005); Popo-ola and Olowookere (2008); Abubakre *et al.* (2010); Foon and Fah (2011)
5	Organisational learning for fraud prevention	Torres *et al.* (2006); Seltzer (2008); Safa and Von Solms (2016); Shah *et al.* (2016)
6	Adaptive Policies, Procedures and Controls	Bierstaker *et al.* (2006); Torres *et al.* (2006); Streff (2009); Adewale *et al.* (2014)
7	Specialist third parties for online transactions to enhance confidentiality.	Tan *et al.* (2002); Goi (2006); Williams (2014)
8	Historical data to determine probability of fraud during each transaction	Fedrizzi (2004); Lamont (2010); Browdie (2012); Abu-Shanab and Matalqa (2015); Grace *et al.* (2016); Crossman (2017)

The table above summarises the literature supporting the strategic factors that were discussed within this section.

2.8.2 Operational Factors

Strict Internal Controls

As a large proportion of fraud is committed by employees who exploit breakdowns in internal controls, strict internal controls has been identified as an effective defence measure for fraud prevention (Sidden and Simmons, 2005). Adetiloye *et al.* (2016) explains that one of the uses of internal controls is to ensure that losses due to fraudulent activities is kept at a minimum. Taiwo *et al.* (2016) also found that the establishment of an adequate internal control system was required for fraud prevention. Research by Akbari (2013) found that internal controls are able to positively affect operational risks for banks and placed emphasis on the importance of adopting controls to mitigate risks. A study by Rahman and Anwar (2014) reiterates this argument explaining that internal controls was identified as one of the most effective techniques for preventing fraud.

It is understood that the majority of fraud is committed by employees who exploit the organisations they work for (Sidden and Simmons, 2005). This is a common risk for banks which requires the implementation of strict internal controls to guard against internal fraud.

Availability of Financial Resources

Given that security measures require resources which usually can be translated into financial value, it is imperative that these resources are made available. Torres *et al.* (2006) explains that organisations should have an information security budget. He highlights that organisations should see security related costs as an opportunity to improve their information security and reputation within a changing risk environment. One of the barriers to adopting best practice for e-banking security is due to limited financial resources available for investing in technology or training (Abubakre *et al.,* 2010). Therefore, banks should endeavour to invest their resources in security to protect their information and customers within the dynamic environment they work in. Unavoidably, resources are limited for all organisations and therefore banks should budget and prioritise their security spend accordingly.

Management & Employees Readiness to Change

Having a proactive approach to security is needed, especially given the magnitude of losses that can be incurred by banks and customers in the event of fraud. One of the findings from a study in Nigeria is the need for more proactiveness in banks (Abubakre *et al.,* 2010). One of the challenges highlighted is that it can take more justification for management to buy into new investments for security, especially when there are low levels of incidents. Therefore, it is necessary to ensure that steps are taken to ensure management and employees understand why changes may be necessary.

Krummeck (2000) suggests that banks must change the culture of how fraud is prevented or detected. The study suggests that fraud prevention should not be limited to one department or team but should be a shared effort from all employees. It is recommended that banks encourage a culture of integrity and show zero tolerance to fraud. One of the ways to encourage employee change is for banks to motivate their employees. Taiwo *et* *al.* (2016) recommends that staff motivation should be a top priority for staff to help keep staff involvement in fraud at a minimum. Incentives such as rewards, bonuses and salary increments are all recommended.

Careful Organizational Change / Change Management

In addition to management support, literate places emphasis on change management. It is suggested that changes should be carried out in a carefully planned manner. Radical change should be avoided as it can result in low employee morale and collapse of traditional service or customer base (Shah, 2009). Therefore, although there is need for change, it should be carefully and strategically implemented to ensure that it achieves the desired impact. Niranjanamurthy and Chahar (2013) argues that the constant technological and business change requires a coordinated approach which leverages algorithm and technology-based solutions. Krummeck (2000) recommends that communication is key to managing change and should encapsulate the use of a wide range of communication channels. This includes messaging systems, training sessions, presentations, management meetings and on the intranet. In summary, e-banking and security are both dynamic topics requiring frequent changes to support new services or protect against new threats. This is attested to by Giles (2010) who suggests that careful management and continuous improvements are required to keep e-banking services secure. Banks should plan for change and ensure its managed in an effective and non-disruptive manner.

Regular Internal Audits

The importance of internal audits on minimising fraud is highlighted by Coram *et al.* (2008) which concluded that organisations with internal audit functions are more likely to detect and self-report fraud than those that don't have an internal audit function. In addition, the research found that organisations that have some in-house internal audit functions are more effective in detecting and self-reporting fraud than those with a completely outsourced internal audit function. However, it has been argued that internal auditors are costlier in comparison to outsourced auditors and may be less independent (Salameh *et al.*, 2011). Olatunji and Adekola (2017) recommended that in addition to frequent audits, auditors should increase the scope of their activities to enhance fraud prevention, particularly on the efficiency of the banks internal control system, risk assessments and system audits. Additionally, Ojo (2017) investigated into the role of internal auditors in Nigerian banks and concluded that the regular review of banks internal controls helps reduce the occurrences of fraud. As internal fraud has been repeatedly identified as a common issue, internal audits may be able to play a role in preventing fraud or identifying actions that may lead to fraud, such as unauthorised access to systems.

Top Management Support

Top Management Support has commonly been identified as a CSF for security related research. This may be due to the need for management to support the introduction of new systems or controls which may also require changes to the modus operandi. Lack of top management support has also been identified as a significant barrier to adopting best practice (Abubakre *et al.,* 2010). Alnatheer (2015) identified top management support to be a CSF after a study to understand information systems security culture CSF whilst Zafar *et al.* (2011) established that executive support was also a CSF for effective security risk management. This indicates that a number of studies have found top management support to be critical for ensuring security. Given that resources are limited, top management support helps ensure that e-banking solutions can receive the required investments it needs (Mutunga, 2013). Epstein (2004) emphasised the importance of involving top management to aid their understanding of any issues and interact with other stakeholders as may be necessary. This implies that top management have an important role to play in e-banking security, which goes beyond making available financial resources.

Strict Customer Data Protection

It is already understood that the security of transactions has an impact in customers' usage of e-banking systems (Haque *et al*., 2009). Security and privacy are at the top of users concerns for internet banking (Lallmahamood, 2007). Therefore, customers are already wary of using e-banking services because of the security of their data. It is imperative that the security of their data is maintained.

The importance of keeping customers' data secure cannot be over emphasised as this closely relates to trust (Datta, 2010). Any violations of this can lead to loss of customers and can affect the banks reputation. Some of the measures adopted to protect customer data include cryptography, digital signatures and certificates which protect against fraud, hacking and phishing (Datta, 2010). Customer data protection helps ensure confidentiality and was highlighted as one of the main safety components for electronic payment systems (Dzemydiene *et al.*, 2010). Similarly, Mahdi *et al.* (2010) also investigated into card not present fraud in banks and recommended the need for banks to utilise technology to protect all their sensitive data.

Responsive Customer Service

One of the factors for preventing fraud for banks is to have a responsive team that will help prevent fraud during vulnerable periods where timing is crucial. This is because stolen cards are often used for fraud within the first few hours of being stolen (Seegar, 2005). Similarly, Balogun *et al.* (2013) emphasised the need for bank employees to be able to quickly react. A quick response can help prevent or limit fraud during the short window after a customer's card or details has been stolen. One of the proposed solutions to address this is to have cardholders' register their cards with a fraud protection plan which allows the administrator to contact the issuers in the event of a reported fraud or theft (Seegar, 2005). In such instance, the administrator's sole responsibility would be to rapidly block the customers' accounts or cards across multiple financial institutions to ensure fraud cannot take place. Whether this is done by a third party or the bank, the objective remains the same, which is to quickly respond to customers and prevent fraud.

To react swiftly to the threats of fraud, banks have started blocking cards where suspicious activities or changes in the customers' pattern are detected. However, this resulted in customers' cards being blocked in the event of simple behavioural changes, resulting in decreased customer satisfaction. More recently, adaptations in technology help ensure that customers are not blocked from using their cards unless there is a high probability of fraud by adopting integrated analytics (Zoldi, 2015). This helps provide the required security whilst also maintaining positive customer relationships.

Security Specialist Team

Organisations should engage security specialist teams to help prevent fraud. The scope of the security specialist team may include physical and information security. Specialist teams can help ensure that the IT security policies are met. In the instances where a team of security experts have not been established for banks, they can be complimented with the use of third-party security providers (Goi, 2006). However, this may be a more resource intensive approach. On the other hand, it may provide the opportunity to have independent views and feedback. In contrast, French (2012) suggests that banks can hire a hacker to be a part of their security team. This will help introduce proactive penetration testing to address any potential loopholes in their systems.

Table 2.3: Summary of Operational Factors for E-Banking Fraud Prevention

No	**Factor**	**Reference**
9	Top Management Support	Epstein (2004); AbuZineh (2006); Torres *et al.* (2006); Abubakre *et al.* (2010); Zafar *et al.* (2011); Koskosas (2011); Mutunga (2013); Alnatheer (2015)
10	Financial Resources	Torres *et al.* (2006); AbuAli and Abu-Addose (2010); Koskosas (2011); Alnatheer (2015)
11	Management and Employees Readiness to Change	AbuAli and Abu-Addose (2010); Giles (2010); Koskosas (2011)
12	Change Management	Shah (2009); Giles (2010); Niranjanamurthy and Chahar (2013)
13	Regular Internal Audits in Banks	Coram *et al.* (2008); Salameh *et al.* (2011); Ojo (2017); Olatunji and Adekola (2017)
14	Strict Customer Data Protection	Rizzardi (2008); Mahdi *et al.* (2010); Dzemydiene *et al.* (2010)
15	Security Specialist Team	Goi (2006); French (2012)
16	Strict Internal Controls	Sidden and Simmons (2005); Benjamin and Samson (2011); Aransiola and Asindemade (2011); Akbari (2013); Rahman and Anwar (2014); Taiwo *et al.* (2016)
17	Responsive Customer Service Team	Seegar, (2005); Balogun *et al.* (2013); Zoldi, (2015)

The table above summarises the literature supporting the operational factors that were discussed within this section.

2.8.3 Technological Factors

It appears that technology will continue to play a pivotal role in e-banking fraud prevention, especially given that the service itself is provided over an electronic medium running on a foundation of IT infrastructure.

Several literatures discuss the importance of authentication systems in securing e-banking services. The security measures discussed include the need for passwords by Johnson and Moore (2007), One Time Passwords (OTPs) and encryption, which is also reiterated by Ganesan and Vivekanandan (2009). In 2004, Hertzum *et al.* (2004) stated that authentication was based on two secrets, one that the user knows and one that they possess. FFIE (2005) suggests that there are three basic factors used for existing authentication methodologies:

1. Something the user knows such as passwords and Personal Identification Numbers
2. Something the user has such as ATM Card or Smart Cards
3. Something the user is such as fingerprints or any other biometric characteristics.

It is recommended that authentication involves a combination of these factors.

Strengthening of Authentication Systems using Biometrics

Given that conventional methods of authentication via usernames and passwords are no longer sufficient (Vandommele, 2010), biometric technology has been suggested as a means of improving e-banking security by stronger authentication. Biometric technology enhances the security levels as it uses a dimension of authentication known as “proof by property” (Dimitriadis and Shaikh, 2007, p.99). It entails using a physical or behavioural attribute of the user for the purposes of authentication. Adetiloye *et al.* (2016) investigated into fraud prevention in Nigerian banks and recommended the use biometrics to control fraud. This type of technology can potentially play a pivotal role in minimising e-banking fraud. Biometrics can be from physical body features or behavioural traits to define levels of distinction. Examples of biometrics include ocular, hand, facial and medico-chemical body features such as body odour and DNA (Adewale *et al.*, 2014).

Research on the potential impact of biometric technology exists and has shown that its deployment to ATM security adds a third layer of security and would certainly reduce the rate of fraudulent activities on ATM machines (Akinyemi et al., 2011). Keystroke Dynamics is a biometric technology that has also been introduced to help fraud prevention. Keystroke dynamics is the process of analysing the way a user types by monitoring the keyboard inputs thousands of times per second and attempts to identify them based on habitual rhythm patterns (Monrose and Rubin, 2000). Ecuador Bank is one of the banks to adopt this technology for its convenience and ability to improve online banking security (PRWEB, 2010). Similarly, the Bank of Utah deployed a keystroke dynamic technology in a bid to strengthen the security of their internet banking service (Hosseini and Mohammadi, 2012). Its ease of setup and minimal inconvenience to customers has made it a good prospect to banks.

Authentication solutions being economically viable

There are many exciting new technologies and solutions being developed such as fingerprint, iris technology, keystroke dynamics and voice recognition. However, Murdoch and Anderson (2010) highlighted that secure authentication solutions need to be both technologically sound and economically viable. Consequently, it is pertinent that such technologies are developed in a form that will be affordable to the banks. For example, research by Adewale *et al.* (2014) found that both bank management and consumers felt that biometrics is the answer to checkmating fraud, but the low level of adoption has largely been attributed to cost. Therefore, a technology with 100% authentication accuracy will be useless to banks and customers if it is not made affordable for the banks to adopt. On the other hand, banks also need to ensure they understand the cost of ownership when adopting security systems. The aim is to meet security requirements whilst keeping operational costs at a minimum (Bai *et al.*, 2012). The costs need to be manageable to ensure continuity and limit the need for banks to transfer such costs to their customers.

Password Security

Password security is frequently used to prevent fraud and remain the first line of defence for most systems (Bierstaker *et al.*, 2006). However, criminals have increasingly become more accustomed to the simple, repetitive or predictable passwords which has led to password-guessing and dictionary attacks (Bellovin and Merritt, 1992). Improved processors and attack tools are shrinking the time required to crack passwords every year (Lemos, 2006). Herley and Van Oorschot (2012) argued that passwords have already been around for longer than initially expected and will remain for some time given their fit amongst known situations. The reality is that even in the scenarios where technologies such as biometric authentication systems are used to access e-banking services, passwords are used as alternates (Tsai *et al.*, 2012). More recent studies have also shown that passwords remain an effective technique for preventing fraud (Rahman and Anwar, 2014). Whilst managing password authentication, it is suggested that they should have expiry dates, restrictions on reuse, and standards on length and strength (Hopkins, 2011).

Javelin (2017) recommends that strong, unique and regularly updated passwords should be used to protect against fraudsters. Strong passwords should contain a multiple words and mixed case alpha-numerics (Lemos, 2006). The minimum length of characters a strong password should contain ranges from 6 to 8 characters based on different literature. It is also argued that passwords that are re-used are also not considered to be strong passwords (Griffith, 2010). Historically, research has found that there are many users willing to trade security for convenience (Tam *et al.*, 2010). Therefore, the study recommended that users are not only informed about why they need to use strong passwords but also the potential consequences of not using strong passwords.

One Time Passwords

One Time Passwords (OTPs) display a time-dependent code that the user will be required to input into the banking interface (Johnson and Moore, 2007). The password is valid for only one transaction or login session (Onomza *et al.*, 2015). Customers are required to request for OTPs each time they want to perform transactions. The OTP can be provided via a hardware device, software, sms or email. The effectiveness of OTPs with restricted periods (between 30-60 seconds) have been reported as significant (Roberts, 2007). OTPs have been reported to be very secure and significantly reduces risk (Hopkins, 2011).

Using Smart Cards for Authentication

Smart cards have provided a convenient but secure approach for customers to authenticate. Smart cards were being looked into since 1985 where it was proposed as new card measures to help prevent fraud (Hyman, 1985). However, it was not until nearly two decades later when the measure started to become more widely adopted due to issues being experienced with magnetic stripe cards. At this point, several countries including Nigeria and the UK started to look at adopting this technology due to the cost of card fraud (Bruno, 2002). There have been studies to compare smart and magnetic stripe cards for some time, specifically with respect to how they can be used to prevent fraud. In addition to the security benefits, smart cards are more durable than magnetic stripe cards as they are not affected by magnetic fields or the type of scratches that would usually prevent a magnetic stripe card from working (Madhok *et al.*, 2002). This coupled with the enhanced security features has made smart cards an attractive alternative to magnetic stripe cards for banks. Similarly, Barker *et al.* (2008) also called for the use of smart cards to help prevent fraud.

Studies have taken place to assess the capabilities of smart cards to further prevent fraud. A study by Malek et al. (2008) found that artificial intelligence using neural networks can be used with smart card platforms to learn behaviours and detect abnormalities. Therefore, further leveraging a smart cards capability to prevent fraudulent transactions from occurring. In contrast, Arnfield (2014) calls for real time technology to prevent fraud arguing that smart cards alone do not lesson the problem of card fraud. However, the study does acknowledge that smart cards do reduce the risk of counterfeit cards.

Multi-Layer Passwords

Rather than relying solely on a single username and password, a secondary system can greatly improve security (Pierson and DeHaan, 2015). Multi-layer passwords require the user to enter 2 separate passwords before they can be successfully authenticated. It is a low complexity cost effective mechanism for strengthening user authentication. Multi-layer passwords are commonly used for online banking services (Vu *et al.*, 2007). Therefore, providing additional layers of checks prior to a user being authenticated. A combination of what the user knows and something the user possesses such as a token has been suggested as effective (Hopkins, 2011). Similarly, Shaji and Soman (2017) recommend the use of multi-layer passwords with other forms of authentication such as biometric technology. It was suggested that the adoption of OTPs and fingerprint biometric technology further strengthen authentication for online banking.

Data Encryption

Encryption refers to the use of mathematical algorithms to code data (Roberds, 1998). An example was given earlier within this chapter regarding the potential implications of not encrypting data. The importance of data encryption is also emphasised by Sun *et al.* (2002), where it states that data encryption is used to help hide any information that may reveal a user’s identity. The encryption and decryption of data is suggested as an important measure in protecting the confidentiality of data and helps against spying during internet banking usage (Niranjanamurthy and Chahar, 2013). Research is constantly being carried out to discover stronger methods to encrypt data. For example, Mannan and van Oorschot (2011) suggested the need for stronger encryption of password data across less trusted devices whilst Ganesan and Vivekanandan (2009) recommended a hybrid model to perform the encryption and decryption processes.

Scalability of Security Systems

The scalability of systems is identified as important due to the need for IT systems to integrate with other systems and cater to the large volume of data which banks are required to process. Veloso *et al.* (2003) explained that due to the high volumes of transactions on a daily basis, banks must have a data mining system which is scalable so that card fraud can be prevented in a timely manner. Moskovitch *et al.* (2009) also called for the scalability of systems, but in the context of biometrics. It was emphasised that that the scalability of security technologies such as keystroke dynamics are very important. Similarly, Bharadwaj *et al.* (2015) highlighted how scalability is a challenge for online biometric learning technologies implying that the systems need to be scalable to be able to offer the additional security benefits associated with using biometric technology for authentication. Although the examples all cover different solutions, there is a common emphasis on the need for such systems to be scalable, to meet the demands of high-volume transactions.

User Friendliness / Usable Security

User friendly interfaces are important features for e-banking services (Aggelis, 2006). While securing e-banking mediums are of high importance, organizations should balance the need for increased security with ease of use to maintain usefulness to the end user

(French, 2012). If not, the customers may end up not using the system and stifle the adoption rate of the solution. Technical measures that are incorporated into security systems are of little value if users are not able to understand the risks and consequences associated with improper use of them (Butler and Butler, 2015). Therefore, its necessary to have a user interface that helps enforce security measures in the most discrete and user-friendly fashion as possible. This is also referred to as usable security.

Usable Security can be seen as the conflict between ease of use and security (Hertzum *et al.*, 2004). It was suggested that the following questions should be asked when ensuring usable security:

- Is the user made reliably aware of and able to successfully perform security subtasks?
- Is the user prevented from making dangerous errors?
- What is the cost of the security subtasks in terms of added user-interface complexity - is there a risk that the user does not feel sufficiently comfortable to continue using it?

It appears that all these questions should be fully considered when developing interfaces for e-banking services. Limited amounts of interaction by the user will help limit the exposure, data and time required to carry out transactions. On the other hand, minimal administration for maintenance enables IT teams to focus on other aspects such as monitoring the IT systems and responding to threats. Hence indicating the importance of user friendliness for preventing fraud.

Integration of Solutions

Integration of systems allows different systems to talk to each other. When looking at it from an e-banking security perspective, it provides an opportunity to link to external systems for additional intelligence. However, the advantages of system integration come at extra costs to organizations (Shah, 2009). Watagase (2005) cited in Akbari (2013) identified system integration as factors influencing operational e-banking risks. This is likely because lack of integration can limit the security capabilities of a system such as the ability to implement transaction monitoring. It has been suggested that integration can be used to achieve enhanced safety and secure e-banking services (Abu-Shanab and

Matalqa, 2015). An example of a scenario where integration helped reduce e-banking fraud was when a bank formed an alliance with a company which provided fraud prevention solutions. Integrating the banks systems resulted in the bank being able to quickly benefit from a leading provider of fraud prevention tools and became more proactive in preventing fraud (National Mortgage News, 2006).

Table 2.4: Summary of Technological Factors for E-Banking Fraud Prevention

No	Factors	Reference
18	Biometrics to strengthen authentication systems	Revett *et al.* (2005); Clarke and Furnell (2007); Foster *et al.* (2009); Moskovitch et al. (2009); Akinyemi *et al.* (2011); Hosseini and Mohammadi (2012)
19	Data Encryption	Sun *et al.* (2002); Ganesan and Vivekanandan (2009); Niranjanamurthy and Chahar (2013)
20	One-Time Passwords	Johnson and Moore (2007); Roberts (2007); Hopkins (2011); Onomza *et al.* (2015)
21	Smart Cards for Authentication	Barker *et al.* (2008); Malek *et al.* (2008); Arnfield (2014); Nilson (2016)
22	Strong Passwords	Bierstaker *et al.* (2006); Tam *et al. (*2010); Hopkins (2011); Rahman and Anwar (2014)
23	Multi-Layer Passwords	Vu *et al.* (2007); Hopkins (2011); Pierson and DeHaan (2015); Shaji and Soman (2017)
24	Artificial Intelligence to work with fraud patters and behaviours to predict, alert and prevent fraud	Bierstaker *et al.* (2006); Malek *et al.* (2008); Hopkins (2011); Wei *et al.* (2013); Arnfield (2014); Abu-Shanab and Matalqa (2015)
25	Scalability of Security System	Veloso *et al.* (2003); Moskovitch *et al.* (2009); Bharadwaj *et al.* (2015)
26	User Friendliness / Usable Security	Hertzum *et al.* (2004); Vandommele (2010); French (2012); Butler and Butler (2015)
27	Authentication solutions being economically viable	Murdoch and Anderson (2010); Bai *et al.* (2012); Adewale *et al.* (2014)

28	Integration of Solutions	Shah (2009); Akbari (2013); Abu-Shanab and Matalqa (2015)

The table above summarises the literature supporting the technological factors that were discussed within this section. Although the review of various literature has exposed factors that have been effective in preventing fraud, the factors needed to be validated in subsequent research methods to assess their criticality before any conclusions could be made. Similarly, the latter phases were used to test the classification and grouping of factors with the involvement of industry professionals. Essentially, the factors presented above were hypothesised CSF that need to be confirmed. The next section synthesis the findings from the literature review and CSF theory to propose a conceptual framework for EBFP.

2.8.4 Conceptual CSF-Based EBFP Framework (version 1)

A framework can be defined as a basis structure underlying a system, concept or text (Oxford English Dictionary, 2007). This provides context of what frameworks set out to achieve, which is a supporting structure or foundation which something can be built upon. A conceptual framework depicts the constructs and variables studied and includes any hypothetical relationships between them. It has been previously highlighted that theory building requires the ongoing comparison of data and theory (Glaser and Strauss, 1967). Therefore, it serves as a good starting point for empirical research providing the basis for hypothesis generation (Robinson, 2002). It involves the synthesis of pre-existing knowledge to form recommendations for action, on how to prevent e-banking fraud.

The structured-case approach by Carroll and Swatman (2000) was used to guide the framework development process. This approach suggests that an initial definition of a framework should be followed, with subsequent refinements as the study progresses along its research process and additional knowledge is obtained. Further details are provided in Chapter 6 where it is further explained how this approach was used for the extension of theory.

Upon completing the literature review, a conceptual e-banking fraud prevention framework was defined to address the research problem. The framework captures the factors identified from the literature review playing an important role in preventing e-banking fraud. As earlier mentioned, the review did not simply identify all factors which were come across, but only those that were common across many literatures. The proposed framework is depicted below.

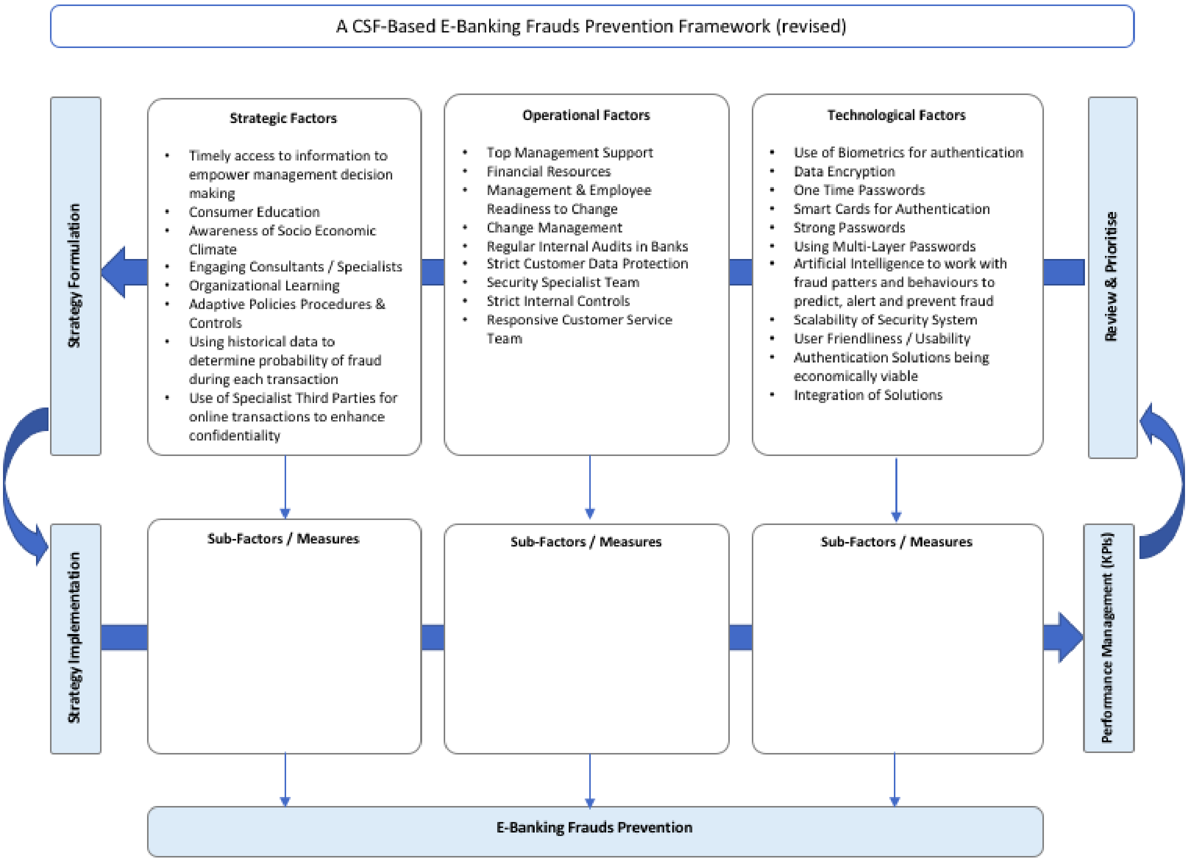

A CSF-Based E-Banking Frauds Prevention Framework (revised)
Strategy Formulation
Strategic Factors
Timely access to information to empower management decision making
Consumer Education
Awareness of Socio Economic Climate
Engaging Consultants / Specialists
Organizational Learning
Adaptive Policies Procedures & Controls
Using historical data to determine probability of fraud during each transaction
Use of Specialist Third Parties for online transactions to enhance confidentiality
Operational Factors
Top Management Support
Financial Resources
Management & Employee Readiness to Change
Change Management
Regular Internal Audits in Banks
Strict Customer Data Protection
Security Specialist Team
Strict Internal Controls
Responsive Customer Service Team
Technological Factors
Use of Biometrics for authentication
Data Encryption
One Time Passwords
Smart Cards for Authentication
Strong Passwords
Using Multi-Layer Passwords
Artificial Intelligence to work with fraud patters and behaviours to predict, alert and prevent fraud
Scalability of Security System
User Friendliness / Usability
Authentication Solutions being economically viable
Integration of Solutions
Review & Prioritise
Strategy Implementation
Sub-Factors / Measures
Sub-Factors / Measures
Sub-Factors / Measures
Performance Management (KPIs)
E-Banking Frauds Prevention

Figure 2.7: Conceptual CSF-Based EBFP Framework (version 1)

The figure above depicts the conceptual framework for preventing e-banking fraud by utilising the CSF theory. Variables were identified from previous literature as discussed within this chapter and categorised into strategic, operational and technological factors for EBFP. The framework deduced a research hypothesis which required validating during subsequent phases of the research. The arrows indicate that all the factors will result in enhanced fraud prevention capability. The proposed framework addresses the following research question.

Research Question 2: What are the factors that have been employed that have successfully contributed to preventing fraud?

The focus for strategic factors relates to banks being able to access key pieces of information early and being able to adapt based on the information available to them. In essence, it highlights the need for banks to be agile by having adaptive policies, procedures and controls (Titrade et al., 2008). Operationally, there is an emphasis to ensure banks have not only adequate controls in place, but also have regular tests to ensure those controls are being adhered to. The UK witnessed up to a 32% decline in fraud within one year, which was attributed to increased customer awareness and fraud detection software in banks (Financial Fraud Action, 2010). This puts into perspective the potential impact of such factors and reiterates the important roles that technological and non-technological factors can both play.

From a technological perspective, user authentication is an area which has been given a lot of emphasis with OTPs and biometrics suggested as important factors for strengthening the process. Other factors organisations should consider include multi-layer authentication and usable technology to ensure security features are of the highest priority. Although technology is an important player in securing electronic channels, it is essential that solutions are economically viable to make them feasible options for banks to adopt.

This section outlines the initial proposal of the conceptual framework. However, conceptual frameworks require the continuous refinement between theory and practice (Lynham, 2000). In alignment with this, the framework was subject to further refinement as the research progressed once further knowledge and insights had been obtained. Updates to this framework are covered in latter chapters of this thesis. Although this proposed framework began to address the initial focus area, there was a desire to conduct further empirical study to validate this, as suggested by CSF theory.

2.9 Chapter Summary

This chapter presented research already existing in the area of this study, e-banking frauds prevention. The chapter also provided an overview of theories that were considered for the study. The literature review helped answer the initial research question:

> **Research Question 1:** What are the security challenges' that banks experience while offering e-banking services?

It was found that fraud has been found as the major challenge to e-banking services. This results in manipulative activities usually result in online banking and card fraud, leading to losses to both banks and customers (Adams, 2010). The review of literature helped develop an understanding on the challenges that banks are faced with in securing their electronic channels. People, allocation of losses, hacking, phishing, card cloning, and identity theft were all challenges that have been highlighted.

A review of theory took place to adopt a suitable theory for achieving the research objectives. The selected theory was discussed, and the theoretical framework was outlined. The review of e-banking and security literature was analysed to identify CSF in e-banking fraud prevention, both technological and non-technological. The findings offered answers to the second research question.

> **Research Question 2:** What are the factors that have been employed that have successfully contributed to preventing fraud?

Although answers had been identified for this question, the next step was to investigate further to determine which of the factors are critical. This was achieved in the subsequent phases of the study. A proposed framework for EBFP was developed in this chapter after a detailed literature review. As highlighted by Boynton and Zmud (1984), CSF include vital issues to current operating activities and its future success. This framework has conceptualised this by outlining the important factors for preventing e-banking fraud. The framework underwent further validation during subsequent research methods and are presented within the relevant chapters of this thesis.

Although the CSF theory has been used in previous studies, the literature review revealed that there are only a few cases in which it has been used for security related research, none of which are specific to preventing e-banking fraud. The next chapter provides details on the research methodology of this study.

CHAPTER 3: RESEARCH METHODOLOGY

3.1 Introduction

This chapter explains the philosophical issues behind the research and the research methodologies that were adopted throughout the study. An introduction and discussion of each of the research methodologies is given within this chapter whilst further details and explanations are covered in subsequent chapters.

It has been stated that there is need for researchers to examine the issues related to research philosophy, approaches and methodologies. Therefore, consideration to a broad range of research methodologies were given by the researcher. There is an argument to suggest that there is no best research method for information systems security (Hirschheim *et al.*, 1996), therefore each research study should be looked at on a case by case basis to adopt a suitable method to meet its objectives. However, the researcher deemed it necessary to understand what methodologies have been adopted for similar studies to understand the strengths and weaknesses that have previously been experienced. The primary objective of research design is to identify the most suitable research decisions relating to the research (Mouton, 1996). In this chapter, the selected research philosophy is presented, and details of the underlying assumptions made for the research are articulated. The research methods adopted are discussed, and a justification for their selection is provided. Finally, the approach taken to plan and execute each of the research methods are also outlined within this chapter.

3.2 Philosophical Issues

This section provides insight into the philosophical background of the research. Creswell *et al.* (2003) recommends that research paradigms are reviewed before proposing research frameworks. The understanding of the philosophical issues underpinning research enhances the ability for appropriate methodologies to be selected (Holden and Lynch, 2004). Therefore, it was paramount that the philosophical classifications were considered prior to the selection of research methods.

3.2.1 Research Paradigms & Philosophy

A paradigm may be described as the basic set of beliefs or assumptions that researchers use as guidance for their inquiry Creswell (1998) cited in (Rocco et al., 2003). It is said that researchers' beliefs on values, knowledge and reality guide their beliefs about research methods (Greene and Caracelli, 1997). A summary of research philosophies considered by the researcher are given below:

Table 3.1: Research Paradigms for Information Systems (Adapted from Khazanchi and Munkvold, 2003; Saunders, 2009)

	Interpretivist	**Positivist**	**Pragmatist**	**Realist (Critical)**
Ontological Assumptions	The social world is produced and reinforced by humans through their actions and interaction	True nature of reality can only be obtained by testing theories about actual objects, processes or structures in the real world	Flux of processes, experiences and practices	Stratified/Layered (the empirical, actual and the real
Epistemological Assumptions	Understanding of social world from the participants' perspective, through interpretation of their meanings and actions	Verification of hypothesis through rigorous empirical testing	Focusses on practical research. Integrates different perspectives to help interpret data	Facts and social constructions Historical causal explanation and contribution
Relationship between theory and practice	Generative mechanisms identified for phenomena	It is possible to discover universal laws	Either or both phenomena and subject meanings can	Knowledge historically situated and transient

	should be viewed as tendencies, which are valuable in explanations of past data but not wholly predictive for the future situations	that govern the external world	provide knowledge	Reality is external and independent
Role of the Researcher	Interactive; the researcher interacts with the human subjects	Objective, impartial observer, passive, value-neutral	Objective or Subjective. Researcher is reflexive	As objective as possible. Tries to minimise bias and errors

The table above highlights the underlying assumptions for the different philosophies. The following sections provide further details on each of the philosophies identified in table 3.1.

3.2.1.1 Interpretivism

The interpretivist paradigm relies on knowledge based on past data. Interpretivism allows close interaction with human subjects enabling questions relating to how and whys' to be addressed (Orlikowski and Baroudi, 1991). Miles and Huberman (1994) argues that interpretivism for research with such collaboration focussing on significant issues achieves high impact on practice, further supporting the decision to adopt the philosophy for research in such an increasingly important topic. Holden and Lynch (2004) argue that researchers cannot distance themselves from the following:

1. What has been observed.
2. The study's subject matter
3. Biasness reflected by characteristics such as the researchers background, status, interests, beliefs, values, resources etc.

Hence, it is argued that the involvement of the researcher should be encouraged (Holden and Lynch, 2004). The interpretivism philosophy usually involves qualitative research methods which frequently require a form of field work, interacting with participants to develop an understanding.

3.2.1.2 Positivism

A positivist approach is associated with the investigator and investigated object being two separate entities and assumes that the investigator can study the object without influencing or being influenced by it (Guba and Lincoln, 1994). In essence, the philosophy states that knowledge comes from the affirmation of theories through strict scientific methods. Positivism usually involves questions or hypothesis being formed and tested via empirical tests to verify them. Crossan (2003) argues that the implications of a positivist philosophy should be that such research must be quantitative. Smith (1998) further explains that positivism assumes objects can be studied as hard facts and relationships can be established via scientific law. The positivist philosophy is commonly adopted in information systems research. For example, research by Alavi and Carlson (1992) which involved reviewing over 900 journals found that empirical articles more commonly adopted a positivist orientation.

One of the major criticisms of the positivist approach is that it does not provide a means to examine human behaviour in depth (Crossan, 2003). Similarly, Alavi and Carlson (1992) stated that positivism denies the perspective that human qualities are beyond the reach of scientific understanding. Therefore, adopting this philosophy may limit the opportunity to understand identified CSFs in depth through interactions with study participants.

3.2.1.3 Pragmatism

Pragmatism enables the researcher to be free of mental and practical constraints imposed by other philosophies. It is the primary philosophy for mixed method research and is an approach to knowledge that seeks to consider multiple viewpoints, perspectives and standpoints (Johnson *et al.,* 2007). It challenges other philosophies by calling for a convergence of quantitative and qualitative research methods. The pragmatist philosophy usually involves the researcher starting with a problem and aiming to contribute practical solutions that can inform future practice (Saunders *et al.,* 2009). Pragmatism rejects the either/or approach to paradigm selection and can help build bridges between conflicting philosophies (Johnson and Onwuegbuzie, 2004). The multiple viewpoints for pragmatism mean researchers can attempt to produce knowledge through employing subjective or objective enquiries (Rorty, 1993).

One of the criticisms of pragmatism is that it can sometimes be seen as an escape route from the challenge of understanding other philosophies (Saunders *et al.,* 2009). Therefore, it was imperative that the different philosophies were considered by the researcher and understood before a philosophical stance was adopted.

3.2.1.4 Realism

Realists to some extent share some beliefs with Positivism and Interpretivism. For example, Realists shares the belief that reality exists outside of human thoughts, similar to positivists. Additionally, realists accept that humans are not just scientific objects that can be studied but also that social beliefs impact their thought and behaviour (Saunders, 2003). Realism can be categorised into two; direct realism and critical realism. Direct realism involves the world being portrayed through personal human senses. Essentially, what you see is what you get (Saunders *et al.,* 2012). However, this is perceived as the more extreme form of realism, and it’s been argued that other factors may need to be considered. Critical realism, portrayed as the less extreme of the two focusses on what is seen and experienced with respect to underlying structures of reality which shapes events (Saunders *et al.*, 2009). The philosophy argues that images or sensations of the real world can be deceptive and usually don’t portray reality (Novikov and Novikov, 2013). Critical realism also sees reality as the most important philosophical consideration (Ackroyd and Fleetwood, 2005). Research for critical realism focusses on in-depth historical analysis of social and organisational structures and how they change over time (Reed, 2005). A range of methods and data types can be used for analysis and the researcher attempts to minimise bias.

3.2.2 Philosophy Adopted & Justification

From an information systems perspective, positivism and interpretivism are the most frequently adopted classifications (Klein and Myers, 1999). However, there have been arguments to suggest that multiple philosophies can be adopted for studies. Newman and Benz (1998) argued that the adoption of a philosophy is not mutually exclusive and that associated research methods can be invoked at different points in time to maximise their strengths. Additionally, a combination of philosophies allows for a more practice-oriented research perspective (Joslin and Müller, 2016). After consideration, the researcher adopted a combination of the positivism and interpretivism philosophies. The researcher believed that this provided an opportunity to utilise the strengths of both philosophical stances for this study over the different phases of the research. An alternative was for the researcher to align to pragmatism. However, the researcher opted to align to the different philosophies at different phases of the research for clear alignment of assumptions and values across the research phases outlined in Figure 3.1.

One of the benefits associated with adopting both positivism and interpretivism is the opportunity to utilise both quantitative and qualitative research methods across the different phases of the research. Firstly, the positivism philosophy is more suited to the context of identifying CSF through an objective, impartial and quantitative approach making it more suited for the first two phases of the research. Once the CSF have been identified, there is need for deeper understanding of how banks achieve the CSF and the activities involved. The researcher felt that aligning to the interpretivist philosophy was more suitable to meet the final phase of the research through involvement and interaction with the banks. Further details on the empirical research for each of the research phases is covered in the next section. Miles and Huberman (1994) argues that interpretivism for research with such collaboration focussing on significant issues achieves high impact on practice. This tied in closely with the desired outcome of the study given the sensitivity of fraud and increasing e-banking adoption.

In summary, a combined philosophical approach was deemed suitable to meet the objectives of the study. It has been argued that a combination of philosophies allows for a more practice-oriented research perspective (Joslin and Müller, 2016). Given that research should not be methodologically led but rather a consequence of the philosophical stance of the researcher, the mixed philosophical approach set the foundations upon which the research methods were determined. Kaplan and Duchon (1988) concluded that there is value in combining research methods for information system research and similarly, this study utilised mix methods to achieve its objectives.

3.3 Empirical Research

Empirical research involves gathering data by direct or indirect observation or experiment. This data can be quantitative, qualitative, or a combination of both (Avison *et al.*, 2008). A summary of the data gathering methods utilised are given in the sub-sections below.

3.3.1 Qualitative Research Methods

Qualitative methods focus on understanding a phenomenon by explaining the meaning of it (Neuman, 2005). It provides methodological tools for deep understanding of meanings associated with complex phenomena (Denzin and Lincoln, 2005). Such research methods involve purposeful sampling, the collection of open-ended data and the analysis of text or pictures (Creswell, 2013). Essentially this research method involves collating participants opinions and experiences via data collection sources such as interviews, observations and questionnaires. This method therefore differs to the traditional commonly used quantitative approach to research which is described in the next section.

3.3.2 Quantitative Research Methods

Quantitative research involves collecting, analysing and interpreting data via surveys and experimental research (Creswell, 2013). Quantitative methods provide scientific answers based on results on sample sizes so that generalizations can be made (Scandura and Williams, 2000). Such studies can involve sampling frames spanning typical, deviant or extreme cases which is determined by the nature of the study (Kelle, 2006).

3.3.3 Mixed Methods and Research Triangulation

Mixed methods can be defined as research that contains qualitative and quantitative approaches. This was later expanded into what is today known as triangulation by Denzin (1978) cited in (Rocco *et al*., 2003). In addition, Remenyi and Williams (1996) encourages the use of both quantitative and qualitative research as a more creative approach to addressing information system research problems.

The researcher adopted triangulation for this study to help improve the reliability of the research. Triangulation enables one method or technique to cross check the results of another (Jankowicz, 2005). Similarly, it has been argued that convergence of findings from two or more methods enhances beliefs that the results are valid (Bouchard, 1976). Triangulation also helps capture a more holistic and contextual portrayal of the area of study (Jick, 1979). Hence, the researcher utilised triangulation in an attempt to achieve such benefits for this research. More specifically, it was used to help identity, validate and deeper understand CSF. This was achieved by using different research methods to arrive at the CSF, but also by engaging different types of respondents such as staff at managerial and non-managerial levels as suggested by CSF theory. Previous studies have highlighted the importance of triangulating data when identifying CSF by involving different stakeholders (Bullen and Rockart, 1981; Boynton and Zmud, 1984). Hence, reiterating its importance in CSF research.

Triangulation is a technique used by surveyors to locate an object by relying on two known points to triangulate on an unknown point (Mertens and Hesse-Biber, 2012). In research, it can be described as the process of combining multiple types of research methods and techniques to look at problems from different point of views.
Patton (2002) discusses four types of triangulation. These are:

- Data sources (data triangulation)
- Different evaluators (investigator triangulation)
- Perspectives to the same data set (theory triangulation), and
- Methods (methodological triangulation)

This study involved the use of two types of triangulation, the first which includes the triangulation of research methods which includes the literature review, survey and case study. The second type of triangulation adopted is data triangulation which was used during the case study research method to use a combination of multiple data sources such as interviews, documents and publications. The evidence from the data sources were used to form findings for the cases which led to conclusions.

Both qualitative and quantitative research have their weaknesses. It has been argued that from quantitative perspective, research may result in insufficient or incomplete theoretical concepts failing to provide explanatory variables (Kelle, 2006). In contrast qualitative research may result in unsuitable selection of cases, therefore leading to issues with the broader applicability of the research.

Adopting multiple triangulation in security related research is not new, Tse *et al.* (2013) employed a similar methodology for research on education in IT security. This involved conducting a survey, interviews and focus groups with bank staff. Triangulation can be used to test reliability and validity of research (Golafshani, 2003). A key feature is its methodological plurism which results in superior research as compared to mono-method research (Johnson and Onwuegbuzie, 2004). Therefore, this approach is adopted to help improve the validity and strength of the research.

3.3.4 Research Methodology Adopted

Research methods involve strategic decisions on data collection methods, procedures and analysis (Creswell *et al.*, 2003). To achieve the research objectives, the research methodology was designed to take place over three phases as depicted below:

Phase 1: Systematic Literature Review
Phase 2: Survey of CSF for E-Banking Frauds Prevention
Phase 3: Case Studies

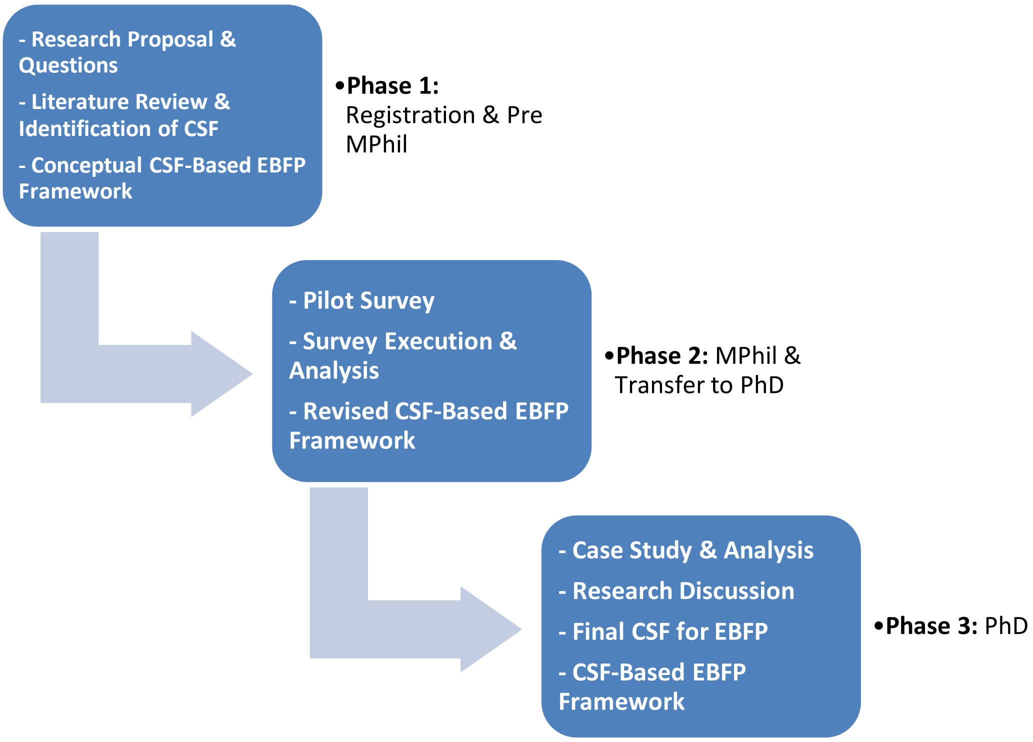

- Research Proposal & Questions
- Literature Review & Identification of CSF
- Conceptual CSF-Based EBFP Framework
•Phase 1: Registration & Pre MPhil
- Pilot Survey
- Survey Execution & Analysis
- Revised CSF-Based EBFP Framework
•Phase 2: MPhil & Transfer to PhD
- Case Study & Analysis
- Research Discussion
- Final CSF for EBFP
- CSF-Based EBFP Framework
•Phase 3: PhD

Figure 3.1: Research Development Phases

3.4 Systematic Literature Review

This research method involved conducting a systematic literature review to understand the current e-banking security environment and where gaps in research existed. This type of review involves critiquing and summarising a body of literature to draw up conclusions on the topic (Cronin *et al.*, 2008). Is has been argued that a well conducted systematic literature review improves the reliability and accuracy of conclusions (Booth *et al.*, 2016). The review type was selected to summarise results from a variety of studies relating to e-banking security and fraud prevention. It was used to provide the reader with a comprehensive background on the topic and to highlight the significance of any new research. Before the commencement of the review, the precise research problem was defined. Literature was carefully selected to ensure relevance and was aided with the guidance of academics in the field who proffered guidance on how and where to identify literature. Details of the review process are given below.

3.4.1 Planning the Literature Review

Planning for the literature review involved considering the literature review types that could be used and selecting a review suitable for the study. Upon selecting the systematic literature review as the type of review to be used, the next step was to define a plan for conducting the review. Cooper (1988) taxonomy of literature reviews was adopted as a framework for carrying out the review. This has also been adopted in previous research and has proved to be an effective method of planning for the review (Randolph, 2009). The taxonomy was used to classify five characteristics of literature reviews. The table below is adapted from Cooper (1988), and provides a summary of the characteristics selected for this research:

Table 3.2: Literature Review Characteristics

No	Characteristic	Categories defined by Cooper's Taxonomy	Categories selected for this research
1	Focus	Research Outcomes Research Methods Theories Practices or Applications	Research Outcomes Research Methods Theories
2	Goal	Integration (a) Generalization (b) Conflict Resolution (c) Linguistic bridge-building Criticism Identification of central issues	Identification of Central Issues Integration: (a) Generalization
3	Perspective	Neutral Representative Espousal of position	Neutral Representative
4	Coverage	Exhaustive Exhaustive with selective citation Representative Central or Pivotal	Exhaustive
5	Organization	Historical Conceptual Methodological	Methodological Conceptual

6	Audience	Specialized Scholars General Scholars Practitioners or policymakers General Public	General Scholars

1. Literature Review Focus

The objective of this characteristic was to define the area of focus for the literature review to help ensure material that is central or relevant to the reviewer is focused on (Cooper, 1988). The focus of this category was to review research outcomes related to e-banking fraud prevention. As the research relates to identifying CSF and defining a fraud prevention framework, there was also the need to review relevant theories that could be applied. It was therefore imperative to cut across the other categories in this characteristic such as the research methods. This specifically aided the identification of suitable research methods that would help achieve the research objectives, as justified in this chapter. Employing the use of a combination of characteristics from the taxonomy is not unusual as dissertation reviews can address all or some of the aforementioned characteristics in addition to the primary focus characteristic (Cooper, 1988; Randolph, 2009).

2. Goal

The goal of the research was to firstly identify the issues involved with the banking security, understand the challenges across the banking industry in preventing fraud. The literature then proceeded to identify existing effective fraud prevention measures employed. Therefore, the key characteristics for the literature review was to achieve generalisation on those factors. However, prior to achieving this, the identification of central issues was also required to provide context with respect to the challenges that had been experienced.

3. Perspective

This characteristic distinguishes how the reviewer may influence the discussion based on their point of view and therefore defining the reviewer's perspective (Cooper, 1988). A neutral perspective was adopted for the literature review. This was to attempt to build no bias into the findings. However, there was an element of judgement required during the identification of fraud prevention factors. This was because the objective of the review was to identify all the key factors that could be used to prevent e- banking fraud. Hence, there was an element of judgement made on the factors/measures discussed in literature. For example, some measures were called or described differently, which introduced a reliance on the researcher to take judgement. However, subsequent research methods were capable of addressing any bias that may have been introduced.

4. Coverage

In terms of the coverage of the review, an exhaustive approach was chosen based on the key words defined. This meant that the literature review examined all available literature from the selected databases. This choice was adopted given the need to sample a broad range of literature globally to obtain a holistic understanding of effective fraud prevention factors prior to the empirical research, which was specifically in the Nigerian context.

5. Organization

Organization relates to how the Literature Review was structured. Historical, conceptual and methodological formats were all formats that were considered. These three formats are the most common formats used to organise literature reviews (Cooper, 1988; Randolph, 2009). The research adopts a methodologically organised format in which it starts with a background of e-banking security followed by a review of e-banking fraud prevention measures before finally discussing the results of the review. However, due to need for the research to expatiate on the factors that were identified, a conceptual format for the review was also used to present the results of the review. This meant that the review findings could be organised according to the identified fraud prevention factors and their categorizations.

6. Audience

This was the final characteristic of the taxonomy literature reviews by Cooper (1988) and sets out to define the audience of the review. The primary audience was defined as the academic staff whom will review the research. However, the review can also be extended to secondary audiences.

3.4.2 Conducting the Literature Review

The review involved carrying out the following stages as defined by (Cooper, 1988). Initially, the study problem statement was defined to pinpoint the scope of the review. Subsequently, literature types, timeliness and suitable databases to find the literature were identified. Key words were chosen and used to find relevant literature. One of the qualities of a good literature review is to gather information from many sources on a particular subject (Cronin *et al.*, 2008). It was therefore necessary for the review information from available books, papers and other available literature from databases to ensure a broad range of sources were exhausted. Details of the key words and databases used are included in Appendix A of this thesis. After the literature was found, the researcher evaluated the literature to ensure relevance and duplicates were removed. The literature was analysed, common themes were identified and discussed.

The review led to the identification of possible CSF for preventing fraud in the e-banking domain. These factors were then investigated further in subsequent phases of the research, starting with the survey by questionnaire.

3.5 Survey by Questionnaire

A survey is a means of gathering information from a sample of individuals about the characteristics, actions, or opinions (Scheuren, 2004). Glasow (2005) explains that surveys can be used for one of the following purposes:

- to answer questions that have been raised,
- to solve problems that have been posed or observed,
- to assess needs and set goals,
- to determine whether specific objectives have been met,
- to establish baselines against which future comparisons can be made,
- to analyse trends across time,
- to describe what exists, in what amount, and in what context.

A summary of the advantages and disadvantages of the survey method are captured in the table below.

Table 3.3: Survey Method Strengths & Weaknesses (Adapted by Stone, 1978; Leedy and Ormrod, 2010; Saunders, 2011)

Advantages	**Disadvantages**
Samples can be chosen to allow generalisations from the defined population	Response formats can may influence respondents to subscribe to statements that they don't endorse.
Ability to collate vast amounts of data directly from the respondents	There could be little willingness or refusal to respond due to suspicion, fear or other resistance
Can be easily administered remotely	Total costs of survey can be expensive because of administration involved
Can be used in combination with other data collection methods.	Response rates are usually low

Remenyi and Williams (1998) explained that a survey can be used for the purposes of description, explanation or hypothesis testing. In this study the survey was adopted as a method to test the hypothesised CSF identified from the literature review. This survey was designed to collate information on the fraud prevention measures that were understood to be critical during the literature review phase of the study. It was designed to provide stakeholders in the banking industry with the opportunity to rate the factors based on their criticality and support the identification of EBFP CSF. It also offered an opportunity for bank staff to propose additional factors which had not already been covered.

Upon selecting the survey method for the second phase of the research, the approach to collecting survey data were considered. Surveys can be achieved by using one of the two common methods for collecting survey data; questionnaire survey and personal interviews. Given the need to extend to a broad reach of targeted respondents, from different locations, the questionnaire survey was selected as the most suitable data collection method.

For this study, a survey was deemed an appropriate quantitative method as it enabled the researcher to reach out to a large sample of e-banking security professionals spread over the Nigerian banking industry. Surveys can also elicit information about attitudes that are otherwise difficult to measure using observational techniques McIntyre (1999) cited in (Glasow, 2005). E-Banking, customer services and IT security staff were identified as the required respondents due to their experience and awareness of issues related to e-banking fraud.

3.5.1 Questionnaire Design

A five-point Likert Scale was adopted for the questionnaire to collect information and measure the criticality of factors. A Likert Scale is a psychometric response scale primarily used in questionnaires to obtain participant's degree of agreement with a statement (Bertram, 2007). Hence, the scales were used to understand levels of agreement with the factors shared with the stakeholders. The recommended number of points that should be used on Likert Scales differ across literature but generally between five to seven-point scales are recommended. Johns (2010) argues that the accuracy of the scales become significantly less when the scale points drop below five or over seven. For this study, a five-point Likert Scale was adopted rather than the seven-point scale. This allowed for a scaling point that can produce accurate results and be less confusing for respondents (Babakus and Mangold, 1992). Additionally, a study had shown that data gathered from a five-point format can be rescaled to a seven-point format if needed by using a simple rescaling model (Dawes, 2008). This therefore made a seven-point scale even less attractive to the researcher.

The questionnaire consisted of three main sections with each of the sections set out to achieve different objectives. The sections are explained below.

- **Respondent Demographics:** This section included questions on the respondents. It set out to provide information regarding the profile of respondents. This enabled an analysis on the impact that the different respondent categories had on factor ratings.
- **Criticality Rating of Factors:** This section organised the factors into 3 sub sections so that respondents could rate the criticality of strategic, operational and

technological factors. This section of the survey made use of a five-point Likert Scale which offered the ability to obtain participant's preferences or degree of agreement with a statement or set of statements (Bertram, 2007). Hence, such scales were used to ascertain the level of agreement with the potential CSF for fraud prevention.

- **Open-ended Questions:** Finally, this section gave an opportunity for the respondents to introduce any additional factors which they deemed critical to e-banking fraud prevention, which had not already been included. Given the profile of the respondents, it was important that it was not assumed that all factors had been covered by the literature review. This provided the opportunity to introduce new factors.

The design of the questionnaire contained an introduction to provide respondents some context and the objective of the survey. At the end of the survey, the contact details of the researcher were also included in case the respondents wished to contact the researcher. The survey was designed and administered online.

3.5.2 Justification of Online Questionnaire Approach

An online questionnaire approach was selected for ease of accessibility to the targeted audience as they were situated across numerous locations. The online questionnaire was chosen as an appropriate means to reach the targeted bank staff and allowed them to complete the survey at their convenience. Access to unique populations, time saving, and reduced costs of the data collection exercise have been identified as some of the main advantages of online surveys (Wright, 2005). The benefits of online surveys have resulted in such surveys being increasingly used in research surveys (Roberts and Allen, 2015). Online surveys make it easier to reach target populations, more convenient for respondents and offer a quick turnaround in terms of the ability to collate survey results when compared to manually completed questionnaires.

The researcher believed that adopting online questionnaires would help reduce the risk of error when compared to the paper-based questionnaires. This was due to the need for paper questionnaires to be translated into digital format for analysis, therefore introducing room for error during the translation process. Also, as the questionnaire employed the use of a 5-point Likert scale, answers could easily be mistakenly altered due to manual input and unknowingly skew the overall results. Therefore, online questionnaires mitigated this risk, eliminated the need to carry out a data entry exercise to capture the results in electronic format before the analysis took place.

Having covered the advantages of adopting an online questionnaire, there was also a need to understand the disadvantages before a decision was reached. The major disadvantage of adopting online questionnaires were related to sample bias and access issues. Thus, the need to consider any potential bias that could come into play. Coomber (1997) explained that previous studies into the demographics of internet users were mainly first world residents, affluent and educated. Therefore, there is a risk of bias with online questionnaires. However, for this study, the potential for bias was understood to be limited due to the questionnaire being targeted at bank staff in Nigeria only with e-banking security experience. All targeted bank staff have access to the internet during their working hours and therefore should have been able to access the survey via the internet.

Another important issue that needed to be considered with online questionnaires was how to provide the prospective participants access to the survey. This is because email invitations to the participants can be rejected, considered as an invasion of the person’s privacy, or can even sometimes prompt the recipient to complain (Wright, 2005). Additionally, there is also the risk that the emails can be considered as spam (Andrews *et al.*, 2003). Hence, the approach to informing targeted respondents may influence questionnaire response rates. Consequently, the following strategy was adopted in a bid to maximise responses.

1. Steps were taken to notify participants as much as possible prior to sending the questionnaire.
2. The emails containing the link to access the questionnaire was channelled via the participant’s colleagues and peers. This was to help decrease the probability of the email being marked as spam. This could also potentially encourage the participants to take part knowing that their colleagues/peers had also done so.

3. The questionnaire was only accessible via a specific link which was shared with the respondents. There was no public sharing or invites via social media to complete this questionnaire. This meant that only those who were targeted would receive the link to gain access to the survey.

In addition to the above, research had found that participants who used a mobile device were quicker to respond to surveys (Cunningham *et al.*, 2013). In the pursuit of timely and high response rates, a decision was made to adopt a survey platform that would be accessible via mobile in addition to the traditional web browser.

3.5.3 Validity & Reliability

The validity of the instrument needed to be considered before the actual execution of the questionnaire. An instrument should only be deemed valid if it is able to measure accurately what it has been designed for (Etchegaray and Fischer, 2010). To ensure validity of the questionnaire, there was need to ensure that the factors selected represented the concept on which the generalisations were going to be made (Kerlinger and Lee, 2000). Content validity was addressed during the literature review phase as it entailed identifying relevant items to the domain of the measurement of interest. This was catered to by the selective approach to identifying literature. The factors measured in the questionnaire were adapted from the findings of the literature review.

Face validity was also a focus at this phase of the research and entailed ensuring that the questions measure what is wanted to be measured. The approach to test the validity in this instance was to introduce a pilot survey to test the instrument prior to the actual survey administration. Designing good survey questions is known to increase the validity of the data collected (Dolnicar, 2013). Therefore, a pre-test of the questions provided an opportunity to improve the questions prior to executing the questionnaire.

Reliability focusses on what extent the survey responses are consistent (Etchegaray and Fischer, 2010). It is expected that survey items for a construct will yield similar answers. The logic being that if the items are similar, the questionnaire respondents will provide similar answers. Some of the tests that can be carried out include Cronbach Alpha, Test-

Retest and Raykov's Coefficient. Cronbach Alpha is the most commonly used test for ascertaining questionnaire reliability (Hogan *et al.*, 2000). This also aligns with the recommendations of Gliem and Gliem (2003) where emphasis was placed on the importance of reporting the Cronbach Alpha values, especially when using Likert type scales. Therefore, assessing the Cronbach Alpha was adopted as a means of testing reliability for the questionnaire.

3.5.4 Data Collection

The data collection process involved disseminating the questionnaire instrument as mentioned above. The questionnaire was administered for a period of 3 months. The strategy for dissemination of the questionnaire was via direct interactions with stakeholders in the banking industry and introductions by referrals from the stakeholders. The number of responses was monitored online, and reminders were sent to help trigger action for either target respondents to complete the questionnaire and/or notify their colleagues asking them to complete too. Overall, a total of 111 responses and a 23.9% response rate was achieved which appeared to be higher than many other CSF related studies. Further details and comparisons to other studies are outlined in Chapter 4.4 of this study.

3.5.5 Data Preparation

Data preparation relates to logging and checking the data that has been collected (Trochim and Donnelly, 2001). This typically involves checking the data for accuracy, transforming and developing the database structure required to analyse the data. This was the first step that happened after the questionnaire had been carried out. For this study, the data was exported from the survey site and then converted into a CSV file so that it could be uploaded into the Statistical Package for the Social Sciences (SPSS) software package. Variables were coded, and the files were saved ready for the data to be analysed.

3.5.6 Data Analysis

After the data collection exercise for the questionnaire had been conducted, the data was analysed using SPSS to obtain descriptive information of the data. This involved identifying the basic descriptive features of the data describing what the data is showing (Trochim and Donnelly, 2001). Data from the descriptive statistics was used to weight and measure the criticality of the factors and the results are presented in the next chapter. This analysis was carried out to form inferences from the data to more general conditions and can be used to investigate questions, models and hypothesis (Trochim and Donnelly, 2001).

For this research, the descriptive and inferential analysis that was carried included:

- Total Responses, Missing Data & Demographic Split
- Mean, Mode & Standard Deviation of factors
- Correlation identification between the factors.
- A reliability test of the scales using the Cronbach Alpha
- Analysis of variances between different respondent groups using Mann-Whitney and Kruskal-Wallis tests.
- Grouping of similar interrelated factors using Principal Component Analysis (PCA)

The next chapter discusses the survey execution in further detail, proving a summary of participation and results from the completed analysis.

3.6 Case Studies

Following the survey, the next phase of the research was to conduct case studies for banks that were involved in e-banking fraud prevention. The case studies have been chosen to follow the survey as it provides the opportunity to focus on specific areas of interest based on the findings of the survey. Voss *et al.* (2002) explained that case studies can be used to follow on from survey research to more deeply examine and validate the empirical results that may have been obtained.

A case study is an empirical inquiry that investigates a contemporary phenomenon within its real-life context, especially when the boundaries between the phenomenon and context are not clearly evident (Yin, 1994). The case study gives the story behind the result by capturing what happened and can be a good opportunity to highlight success or challenges (Neale *et al.,* 2006). Case studies have been described as one of the most important research methods which have been used for many years over a variety of disciplines (Shen, 2009). One of the advantages of case study research is that it provides the ability to embrace multiple cases consisting of quantitative and qualitative data whilst embracing multiple research paradigms for theory development or theory testing (Dooley, 2002). It is therefore a research method that can contribute to a variety of studies due to its ability to add value.

The case study approach could have been used as a suitable research method for the 2nd phase of the research as an exploratory study rather than in the 3rd phase of the research. However, given the need for a deepening understanding of the identified CSF, the case study was more suited for the third phase of the research after the CSF had been identified. There is a stereotype that case studies should be used in the exploratory phases of the research only. However, there is evidence to strongly suggest that the stereotype is not correct (Yin, 1981). More recently, Yin (1994) suggests that case studies can be used for the following instances, which are relevant to this research:

- When there is need to focus on individual actors or groups of actors, and seek to understand their perceptions of events
- When there is need to highlight specific events that are relevant to the case

Consequently, the case study was selected as an appropriate method for meeting the objectives of the third phase of the study. Additionally, a multiple case study approach was adopted due to the need to describe and explain the CSF by engaging multiple banks for data triangulation. Miles and Huberman, (1994) stated that this approach enhances the researcher's ability to determine the relevance and applicability of results, thereby supporting generalisations to be made.

Prior to commencement of the case study, it was also important for the researcher to understand the limitations of case studies. One of the notable limitations was that there had been arguments to suggest that it is difficult to justify making generalisations from a limited number of samples because case studies are limited to relatively low numbers. Therefore, suggesting that case studies alone may not be suitable to generalise CSF. However, case studies provide the opportunity to use qualitative and quantitative research methods, allowing triangulation of data from multiple sources of evidence (Yin, 1994). Therefore, to counter this argument, the researcher used case studies to further understand findings from the quantitative phase of the research which was the survey of bank staff.

3.6.1 Case Study Approach

Case study research can be achieved by using either quantitative, qualitative or even both types of research. Data collection techniques such as observation, document analysis, surveys, interviews and Delphi can all be employed. The data for case studies was collected using a combination of interviews, examination of internal documents, annual reports, and material available online. Literature from Dooley (2002) and Yin (2003), whom are both well-known case study researchers were used to guide the researcher through the case study process. The following approach was adopted:

1. Defining the Research Questions
2. Select cases and determine data gathering and analysis techniques
3. Prepare to collect the data
4. Collect the data
5. Evaluate & Analyse the data
6. Prepare the report

Insights into how each of the six steps were applied to this study are further elaborated below.

3.6.2 Defining the Research Questions

The first stage focussed on identifying the research questions that needed to be answered using the case study methodology. For this study, the research questions had already been identified as outlined in Chapter 1. Appropriate research methods were subsequently identified to attempt to address all the research questions. The following table provides details on the applicable research questions which were addressed by the case study.

Table 3.4: Case Study Research Questions

Research questions	**Objective of Case Study**
Question 4: Which of the factors are the most critical in ensuring the successful prevention of e-banking fraud?	The survey findings ranked factors based on their criticality for preventing e-banking fraud. These factors were identified in the literature review phase of the study. However, the survey included an open-ended question to allow the respondents to indicate whether there were additional CSF based on their experience. It resulted in the introduction of new factors which needed to be validated during the case studies.
Question 5: How do banks achieve the identified CSF to prevent e-banking frauds?	During the literature review phase of the research, some activities ralating to fraud prevention were mentioned. However, the focus during that phase of the reseearch was to identify those factors that were crtiical for e-banking fraud prevention. Once the CSF had been identified, there was further need to understand how banks can meet the CSF. The case study was used to understand the key activities required to achieve the CSF.

3.6.3 Case Selection & Data Gathering

3.6.3.1 Case Selection

A common criticism of the case study research method is the dependency on a single case and that it is very difficult to generalise with a single case or small number of subjects (Zainal, 2017). To try and address this, this study adopted a multi case approach which replicated the case study design for each of the cases. It has been found that for this approach, three or four cases are sufficient to develop explanations or synthesis across cases (Yin, 1981).

A total of four banks were included for the case study. In terms of sampling, Voss *et al.* (2002) suggested that samples can be purposeful or opportunistic. It is also recommended that cases are selected for theoretical reasons, also known as theoretical sampling (Eisenhardt, 1989). Cases to be studied are usually chosen for various reasons ranging from being highly effective, not effective, representative, typical or of special interest (Neale *et al*., 2006). For this study a purposeful sample of banks were selected comprised of 3 banks that offered a similar variety of e-banking services to customers. An associated benefit of this approach is that it enhances the generalisability of the theory (Gersick, 1988). Additionally, a special interest case, the regulatory bank in Nigeria was selected due to its active role in working with banks to prevent fraud over their e-banking services.

3.6.3.2 Data Gathering Technique

Semi-structured interviews were conducted to staff from each bank to provide further context on the CSF for EBFP and understand the key activities carried out for each of the factors. Semi-structured interviews were deemed to be appropriate in this instance as it provided the opportunity for probing into the issues and obtaining personal views as suggested by Gray (2004) cited in (Kajornboon, 2005). In addition, there were new CSF that arose from the survey phase of the study which required further investigation. Although the interviews represented one of the primary sources of information, it was one of multiple data collection techniques employed.

An underlying principal of case study data collation is triangulation, using a combination of methods to study the same phenomenon (Voss *et al.*, 2002). To achieve this, alternative data sources involving documentation, archival records and other available online media were also used. The following table provides a summary of the evidence types used, summarising their strengths and weaknesses.

Table 3.5: Sources of Evidence for Case Study (Adapted from Yin, 2003)

Source of Evidence	Strengths	Weakness
Documentation	• stable - repeated review • unobtrusive - exist prior to • case study • exact - names etc. • broad coverage - extended • time span	• difficult to retrieve • biased selectivity • reporting bias - reflects author • bias • access - may be blocked
Archival Records	• same as above • precise and quantitative	• same as above • privacy might inhibit access
Interviews	• targeted - focuses on case study topic • insightful - provides perceived causal inferences	• bias due to poor questions • response bias • incomplete recollection • reflexivity - interviewee expresses • what interviewer wants to hear

Expectedly, each of the sources had their weaknesses which further justifies the rationale of using multiple data sources, in-line with the triangulation theme of the research. Additionally, it provided the researcher with an opportunity to take measures that may help avoid some of the weaknesses. For example, since the researcher knew that documentation may be difficult to retrieve, it was also requested as part of the interviews in an attempt to increase the likelihood of obtaining relevant documents.

3.6.4 Preparation to Collect Data

To obtain the desired results from the interviews, it was essential that the right people were involved. As recommended by CSF theory and outlined previously in chapter 2, both management and non-management staff were targeted. The strategy adopted for selecting interviewees was to identify a gatekeeper for each bank. The gatekeeper helped identify the most suitable interviewees, ensuring they had been briefed on the research and where possible, also arrange for the interviews. As the researcher understood the banking industry and potential challenges associated with achieving the desired level of participation for a sensitive topic, contacts that were known were approached to help speed up the process. In addition, the gatekeepers were also involved in the identification of an alternative stakeholder from the same stakeholder group where multiple attempts to interview a targeted stakeholder was unsuccessful. After having identified the required stakeholders, contact was made via phone, email or in person, and appointments for the interviews were scheduled.

3.6.4.1 Ethical Considerations

Prior to carrying out any data collection exercises, a formal ethics approval in accordance with the University's procedure was obtained. This is now a common approach adopted in many British universities who have established ethics committees to offer ethical guidance for research (Israel and Hay, 2006). The application process entailed completing an ethics approval form which covered a variety of ethical considerations and then sharing supporting documentation such as data collection instruments with the university for review and approval. This not only ensured ethical considerations were made prior to the collection of data, but also provided a level of comfort to the banks that were approached. The table below summarises the ethical risks and how they were addressed by the study

Table 3.6: Ethical Risks & Mitigation

Risk Item	Relevance	Mitigation
Fieldwork /Travel Risk: This covered the risk associated with the researcher collecting data in Nigeria. Some of the risks considered were in relation to the following: 1. Risk of Riot or Unrest 2. Risk of Attack Whilst Working Alone	The data collection activities took place in Nigeria. Therefore, an assessment of the location was required to ascertain the level of risk and ensure adequate mitigation was in place prior to the researcher travelling.	The following was adopted as mitigation activities for the researcher: 1. Stay vigilant and current with the news. Also, keep in close communication with supervisors 2. Do not carry valuables and large sums of money unless absolutely necessary. Also, the researcher would dress appropriately to fit in with the crowd

3. Risk of Dehydration (due to hot climate)		3. Drink plenty of water and stay in well ventilated areas as much as possible.
Case Study Participation: This related to risks such as non-response or delayed response by participants or banks	Given that the research data collection period was time bound, there was a risk that targeted participants and case study banks may delay the research timelines or limit the amount of data collated.	• Introduction letters with information sheets were used to provide the participants with a brief on the research, their level of engagement required and how they could contact the researcher. This was used to help provide context, obtain consent and instil confidence.
Participant Anonymity: There is a risk that the anonymity of participants may be compromised.	As the research methods involved interacting with human subjects and banks, there was a risk that the anonymity of participants may be compromised.	• Only data necessary for the study was collected. This resulted in a limited number of demographic related data collected. • Information collated was anonymised so that the identities of individuals are not revealed.
Maintaining Confidentiality: There	This study focuses on the sensitive topic of fraud.	• Data was captured electronically as much

is a risk that confidentiality of the information or data collected may be compromised	Data relating to fraud challenges and existing security measures were required. Hence, there was a risk of compromising confidential data which needed to be mitigated.	as possible reducing the risk of confidential paper-based documents being left unsecured • Data and information collated in paper form from interviews were kept locked away. • Computer files were only accessible with a password.

From the table above, the risk items cover broadly two areas, firstly the risks associated with the researcher travelling to Nigeria for the data collection exercise, and secondly the risks associated with the processing the data collected.

The data collection location for the study was a concern as the researcher was required to be physically in Nigeria. Consequently, a thorough risk assessment and mitigation actions were planned. The researcher submitted the output of the risk assessment to support the ethics approval application, which was subsequently approved. One of the mitigation actions resulted in the case study interviews being held at the bank's locations rather than a location designated by the researcher as initially planned. From a security perspective, bank locations were deemed to be more appropriate locations for the interviews to take place. Additionally, there were other benefits such as the location being more convenient for the bank staff whilst providing the opportunity to be introduced to additional staff who may have useful information.

It is recommended that researchers tailor the data collection methods to best suit the sensitive of the research topic (Li, 2008). Given that fraud prevention is a sensitive topic, it was necessary to engage and interact with the participants to collate the data. This helped ensure the participants understood the objectives or the research, why their inputs were required but also to reassure them that confidentiality would be maintained.

3.6.4.2 Anonymity of Cases

Given the need to guarantee privacy of the banks participating in the research, the names of the banks and participants of the interviews are not disclosed in this thesis. This is necessary given the nature of the research and sensitive data that was collated and was the basis on which the banks had agreed to participate. Therefore, the data analysis will not refer to each bank by their name but rather a code name. This is not new to research that involves sensitive information. For example, Kryukov and Strauss (2009) withheld the identification of participants for fieldwork that was carried out for a similar study. Formally informing the banks upfront that this would be done was important to obtaining their buy-in and consent to participate in the study.

3.6.5 Data Collection

This was done by firstly writing to the banks to inform them of the research and its objectives. The banks were then approached to agree on the modalities for interviews and to obtain relevant documentation that could be shared.

3.6.5.1 Conducting the Interviews

Interviews were conducted via either face to face, phone or video calls with the stakeholders at scheduled times. The variety of options helped ensure optimum cooperation of the participants. The semi-structured interview method provided the participants the opportunity to express their opinions freely while maintaining the same interview structure for all participants. The interview approach allowed the discussions to be focussed around the identified factors whilst also allowing for other emergent themes to develop (Jankowicz, 2000). Therefore, aligning with approaches from previous studies.

The criteria for the interviewees were to interview staff in roles that were involved in e-banking services and its security. From previous literature, it was understood that these roles were typically IT, audit, customer services and risk management related roles. However, the researcher also allowed the banks to determine those that may be best to interview based on the background of the research that had been shared with them.

Additionally, the researcher reviewed those that had been proposed to ensure a mixture of interviewee experience were covered, given that the survey found that there were slight differences in terms of the factor ratings for the different categories of respondents. A total of 29 interviews took place in total for all four case study banks. The researcher provides a summary of what transpired through the case study process in Chapter 5 of this thesis.

The interview was organised to start with an introduction of the interviewer followed by a brief on the purpose of the research, the purpose of the interview and the format of the interview. Questions were then asked, with further probing questions being asked where appropriate. Given that there were varying roles involved, it was important that this was understood, and the interviewees were given enough opportunity to provide input based on their areas of expertise. Multiple interviews were conducted to increase the likeliness of validity, consistency and minimise bias (Yin, 1994). The duration of the interviews ranged from 40 minutes to a maximum of 1 hour 30 minutes for both management and non-management interviewees.

Table 3.7: Summary of data collection from secondary sources

Organisation	Types of secondary data used for triangulation
CSB-1	• Annual report for the years 2015 & 2016 • Whistle-blower Policy and Procedure Documents • Reference material accessed from the bank’s website regarding e-banking security • Security Tips Guidance Document • Social Media Pages - Facebook, Linked-In
CSB-2	• Annual report for the years 2013, 2016 • Whistle-blower Policy • Reference material accessed from the bank’s website regarding e-banking security • Fraud Prevention Security Tips Video • Account & Internet Banking Opening Terms and Conditions • Online Transfer Advice • Social Media Pages - Facebook, Linked-In

CSB-3	• Annual report for the years 2014, 2016 & 2016 • Whistle-blower Policy • Card Replacement Request Form • Two online published articles • Account Opening & Merchant Application Form • Reference material accessed from the bank’s website regarding e-banking security • Fraud Analysis Presentation • Account & Internet Banking Opening Terms and Conditions • Email Exchanges • Social Media Pages - Facebook, Linked-In
CSB-4	• Annual report for the years 2014, 2015 & 2016 • Neff Annual Reports 2014, 2015 & 2016 • Bank Supervision Annual Report 2015 • 6 Circulars related to E-Banking Fraud, Authentication & BVN • Guidelines on operations of electronic payment channels in Nigeria • Regulatory framework for bank verification number (BVN) operations and watch-list for the Nigerian banking industry • Interim report of the committee on ATM fraud prevention and resolution • Reference material accessed from the bank’s website regarding e-banking security

3.6.5.2 Data Collection Exit Criteria

Although the data collection objective was to extract as much useful data necessary over the course of the exercise via the defined data sources. It was also important to define what the data collection exit criteria was. Exit criteria decisions should involve both theoretical and practical considerations (Dooley, 2002).

There are four theoretical criteria to determine when it is appropriate to end data collection. This includes the exhaustion of data sources, saturation of categories, emergence of regularities and finally overextension (Lincoln and Guba, 1985). Time and Budget are practical constraints that also need to be considered (Dooley, 2002). This is not only a criterion that may end data collection but may also restrict the data collection scope or strategy in the first place.

The exhaustion of data sources as an exit criterion was less likely for this study given the large number of stakeholders in the banking industry coupled with the time constraints of the research. Additionally, given the sensitive nature of the research topic and the data involved, it was expected that not all documentation and confidential fraud related statistics would be accessible, especially where the banks feel exposing this data could affect their reputation. However, this was a risk accepted by the researcher and had also been highlighted earlier as one of the weaknesses when working with archival or documentation data sources.

The realistic exit criteria to end the data collection was therefore when the emergence of regularities was achieved. This is defined as the point where there are sufficient consistencies in the data providing insight into whether the data from the phenomena represented by each construct occurs regularly or occasionally (Dooley, 2002).

3.6.6 Case Analysis

After the data collection had been completed, the next step was to analyse the data. A combination of analysis within-case and cross-case analysis was carried out as suggested by (Eisenhardt, 1989). George and Bennett (2005) also argues that case studies can be used to explore causal relationships behind correlations and patterns that may have previously been observed. This was used to further understand some of the challenges experienced in preventing e-banking fraud and their causes.

Within case analysis was carried out to analyse the responses received from each case study bank. This involved comparing the responses from the interviews and other secondary data obtained. An array or display which presents data systematically which allows conclusions is recommended as a useful starting point (Voss *et al.*, 2002). Once this had been done, possible explanations and causality was looked at. One of the drawbacks of within case analysis is the prospect of analysing a large volume of data because the research problem is typically open ended (Eisenhardt, 1989). The researcher therefore was wary of this and attempted to find the right balance.

Cross case analysis can be used when there are multiple case studies available and an inquiry has identified one or a few critical factors (Yin, 1981). Cross-case analysis was used to compare the outcomes of the cases as it was a means of analysing multiple cases. According to Yin (2013), the findings using this approach are likely to be more robust than having only a single case. Voss *et al.* (2002) highlights that the systematic search for patterns across the cases is key in case study research. During this phase, quantitative analysis through tabulations and word tables were also included to display data from the individual cases whilst also aiding the comparison processes across the cases.

Qualitative data analysis usually involves identifying key elements in data which are also referred to as themes and may enter the analysis before or during the study (Ayres *et al.*, 2003). In this study, a combination of both took place with the CSF identified forming the themes of discussion during the case study. However, the analysis approach also considered any additional themes that emerged. Equally important was that the analysis allowed the study to not follow the shortfalls as highlighted by many other research studies where qualitative research fails to go beyond the identification of lists or categories.

3.6.7 Preparing the Report

Yin (2013) advises that multi-case reports can be documented in a variety of options which involve discussing each of the cases in individual chapters, discussing them all in one chapter or introducing a hybrid approach. The option to discuss all cases in one chapter was selected which allowed for information from the individual cases to be dispersed across different sections of the report. This format was selected to provide ease of readability and comparison across cases. As suggested as an option for this approach, summary information for each of the individual cases was included to provide further context prior to the main content.

3.7 Summary of Research Process

The research design process helps anticipate the most suitable research decision for the study (Mouton, 1996). Hence, this was an important milestone for the study. This chapter not only documents the approach taken for conducting the research but also captures the reasoning for the choices the researcher had made.

In terms of the research philosophy, the research was based on positivism and interpretivism. This approach led to the researcher utilising mixed methods to not only identify CSFs but also draw from participants' knowledge to deepen the understanding of factors after they had been identified. Methodological triangulation was adopted involving quantitative and qualitative methods at different phases of the research. Benefits included the opportunity to address shortcomings of the survey as qualitative research helped add further substance to the factors via interactions with banks.

The research methods were selected based on the objective of the research phase and the research questions that needed to be addressed. The first phase of the research involved carrying out a systematic literature review. This allowed the researcher to further understand the challenges associated with e-banking fraud and more importantly, identify factors that have been effective in preventing fraud. Subsequently, the study engaged with industry professionals and banks with research methods that aligned with the researcher's philosophical stance. The table below is adapted by Yin (2003), and summarises the research strategies adopted for the subsequent phases of this study:

Table 3.8: Phase 2 & 3 Research Strategy (Adapted by Yin, 2003)

Research Phase	**Research Method**	**Possible forms of Research Questions**	**Form of Research Question for this research**	**Focuses on Contemporary Events?**
2	Survey	Who, What, Where, How Many, How Much	Where, How Many, How Much	Yes
3	Case Study	How, Why	What, How	Yes

The survey was used to solicit the views of people working in the banking industry to rate the factors in terms of their perceived criticality. Given that the literature review was based on a broad range of fraud and e-banking security literature, it was necessary to provide bankers and security experts a first-hand opportunity to confirm and rank the factors based on their e-banking experiences. To administer the survey, an online survey questionnaire approach was adopted given its suitability to reach out to a targeted set of respondents spread over different locations in Nigeria. Analysis of the questionnaire data was done using SPSS. The analysis involved descriptive statistics which reviewed the data quality, reliability, mean and standard deviation amongst others. Additionally, inferential analysis involved applying the Principal Component Analysis to appropriately group similar interrelated factors.

The final research method involved carrying out case studies. This provided the opportunity to validate findings from the survey and obtain information on "hows" for each of the factors. As recommended by Yin (2003), case studies are appropriate for the explanatory phase of an investigation and therefore deemed as a suitable method for the final phase of the study. Data obtained whilst engaging with the banks were analysed using within-case and cross-case analysis. The structured case approach was used to critically analyse findings comparing them with related literature before further revisions of the framework were made.

Overall this chapter has summarised the research methods that were adopted for the study and the sequence in which they were carried out. Previous studies and literature related to research methods helped the researcher determine the methodology to identify EBFP CSF. Each of the methods were important in attaining the research objectives and provided the opportunity for the CSF theory to be extended by applying it to e-banking fraud prevention, specifically in the context of the Nigerian Banking Industry. Findings from each of the remaining phases of the research are outlined within the subsequent chapters of this thesis.

CHAPTER 4: SURVEY ANALYSIS

4.1 Introduction

This chapter summarises the findings from the questionnaire survey phase of the research. It starts by providing an overview of the pilot study which was carried out and the summary from the exercise. Changes adopted from the pilot are outlined and a brief narrative of the survey execution was discussed.

The results of the survey are discussed beginning with the response rates and descriptive statistics, highlighting which factors were rated with the highest criticality. Outputs of the additional analysis carried out such as correlations, Kruskal-Wallis and Mann-Whitney tests are discussed. Finally, the results of the Principal Component Analysis are discussed and the components that were formed are presented. To conclude the chapter, the conceptual framework for EBFP is refined.

4.2 Overview of Survey Instrument

The questionnaire survey was developed to assess the criticality of the fraud prevention factors that were identified during the first phase of the research. The questionnaire was structured into three sections; respondent demographics, criticality rating of factors and open-ended questions at the end for the participant to provide any further insights. It was designed using an online tool for questionnaires administration. Further details of the questionnaire design are provided in the previous chapter.

4.3 Survey Pilot Study

4.3.1 Pilot Questionnaire Process

The research methodology section of this thesis referred to the pilot survey which was carried out prior to the administration of the survey questionnaire. The pilot was conducted to evaluate the comprehension, relevance and length of the set of questions. A checklist adapted from Iarossi (2006) for pilot survey feedback was tailored for the study to ensure the feedback could address the pilot objectives (Fishman *et al.*, 2010). The contents of the feedback form included questions relating to the objective, length, comprehension and how it had been structured. The feedback form that was used for the study is included in the appendix of this thesis.

The questionnaire and feedback forms were sent to 20 participants. The composition of the respondents were academics, research students from similar fields and working professionals. Feedback was received by 12 out of the 20 subjects giving a response rate of 60%. The feedback was received in the space of 3 weeks. Although additional responses could have been obtained, a decision was made to progress the research using the feedback that had already been obtained due to time constraints. Sheatsley (1983, p.226) states that "It usually takes no more than 12–25 cases to reveal the major difficulties and weaknesses in a pretest questionnaire". Although the responses were at the lower limit, this suggested that the feedback received was sufficient to assess the quality of the survey and its suitability for administration.

4.3.2 Pilot Questionnaire Findings

Highlights from the pilot survey results were that 100% of the respondents believed that the survey wording was clear, had suitable answer choices and made use of appropriate headings. Although this was positive, there were improvement points that had been suggested. The feedback was reviewed, and a decision was made on what actions could be taken to address each of the observations. The identified areas for improvement along with the actions taken are covered in the table below.

Table 4.1: Pilot Survey Feedback & Actions Taken

No	Observation	Actions Taken
1	The length of the survey was too long and may discourage respondents	Questions which were felt to have little impact towards addressing the research questions were removed.
2	The sections needed to be clearer	A brief introduction was included for each section explaining its purpose.
3	A more articulate introduction to the survey should be provided	The survey introduction was revisited and expatiated.

4	Responder demographics contained sensitive information which may discourage respondents	Some questions such as age, current job & role were removed from the survey.

The survey instrument was revised to incorporate the recommendations before commencement of the actual survey. Whilst revisiting the survey structure, literature from Henning *et al.*, (2009) was come across which identified the position of open-ended questions as key to the response rate of the question. Previous research had concluded that a 90% response rate was achieved when the open-ended questions were placed at the beginning of the survey in comparison to the 61% response rate that was attained when the open-ended questions were placed at the end of the survey. After some deliberation by the researcher, a decision was made that it was more beneficial to retain the open-ended question at the end of the survey. This was because the only open-ended question was designed to identify additional factors or experiences that help prevent e-banking fraud that were not captured in the other sections of the survey. Therefore, moving such a question to the top of the survey would increase the likeliness of the respondents mentioning the factors that were already included in the other sections.

It is generally agreed that a pilot survey can reveal deficiencies in the design of a proposed experiment providing an opportunity to address them before time and resources are expended on large scale study (Altman *et al.*, 2006). In this case, the pilot not only highlighted deficiencies but also demonstrated the survey strengths, providing confidence of its suitability and readiness for administration.

4.4 Survey Execution & Response Rate

The survey was sent to 23 banks in Nigeria. The method of distribution was through introduction by members of staff of the Central Bank, the apex regulatory bank in Nigeria. The survey was specifically targeted at bank staff and stakeholders who work with e-banking security. They were also asked to forward to all suitable staff to complete. Given that one of the weaknesses of adopting online questionnaires is that it may be accessed by a broad range of respondents which may not necessarily be those targeted, a decision was made to only share the survey link with targeted banking personnel.

The planned duration of the survey was 1 month. However, due to the initial low number of responses, the duration was extended to 3 months. Reminder emails, text messages and phone calls (where the contact details were known) were also used to help increase the number of responses. Feedback from the contacts were that there were a limited number of staff they could engage to complete the survey given the need for familiarity and experience in e-banking security. Interactions with the bank staff revealed that the limited number of responses was partly due to the targeted audience that was specified. Although this restricted the number of responses that could be obtained, it helped ensure the quality of the responses was not compromised.

A total of 111 responses were received over the survey period. From this, 1 of the responses was a duplicate submission. Therefore 110 of the responses were usable and taken forward for analysis. A total of 20 people was targeted from each of the 23 banks. This indicated that a response rate of 23.9% was obtained. In comparison to previous CSF studies, (Shah *et al.*, 2007) achieved a response rate of 22.4%, Osei-Kyei *et al.* (2017) achieved 14% whilst Chow and Cao (2008) achieved an extremely low 2.4%. In contrast, Lopes and Oliveira (2015) achieved a very high response rate of 80%, indicating that there was a broad range of response rates that had been obtained from previous studies. Overall, the response rate obtained appeared to be higher than previous CSF studies that involved data collection using surveys. Upon collecting the data, the next step was to transform this data into useful information to obtain valuable insights from the results.

4.5 Data Analysis

This section provides an overview of the statistical analysis that was applied to the data obtained from the survey.

The factors that were listed in the survey were ranked using their mean scores to see if there was a consensus regarding the criticality weighting of the factors. The results indicated large differences between the highest and lowest rated factors implying that those at the top are more critical to e-banking fraud prevention than the others. Additionally, analysis was carried out to understand whether there were statistically significant differences in ratings between the categories of survey respondents. Mann-Whitney tests were applied to differentiate between the two gender categories, whilst Kruskal-Wallace tests were used to compare variances of the different categories of experience that the respondents had. The final part of the analysis was to perform factor analysis on the variables to group the factors into different categories.

4.5.1 Data Coding

The statistical analysis was carried out using SPSS, a popular statistical software package for the analysis of empirical data. The software allowed data to be imported, prepared, analysed and the outputs extracted for evaluation. All variables for the survey had already been named by the survey tool that was adopted. However, the names were not suitable due to their length and lack of readability in SPSS. Therefore, the variables were coded with a prefix of either S, O or T depending on whether the variable related to Strategic (S), Operational (O) or Technological (T) factors. This was then followed by the variable number which started at 1 for the first variable and then increased incrementally by 1. In addition, all the variables were formatted as either numerical or strings. Finally, the data fields were categorised into nominal and ordinal data categories.

4.5.2 Descriptive Statistics

The table below provides insights into the profile of the questionnaire respondents summarizing the frequency of responses, gender and e-banking security experiences.

Table 4.2: Frequency and Gender of Respondents

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Unknown	1	.9	.9	.9
	Female	44	40.0	40.0	40.9
	Male	65	59.1	59.1	100.0
	Total	110	100.0	100.0	

The table above provides a summary of the total usable responses and the respondents gender. Although the larger proportion of respondents were male, 40% of the respondents were female. Capturing such data enabled further analysis to understand the differences in ratings per gender and experience categories. Further details are covered later within this chapter. The pie chart below summarises the distribution of respondents over the different ranges of work experience with e-banking security.

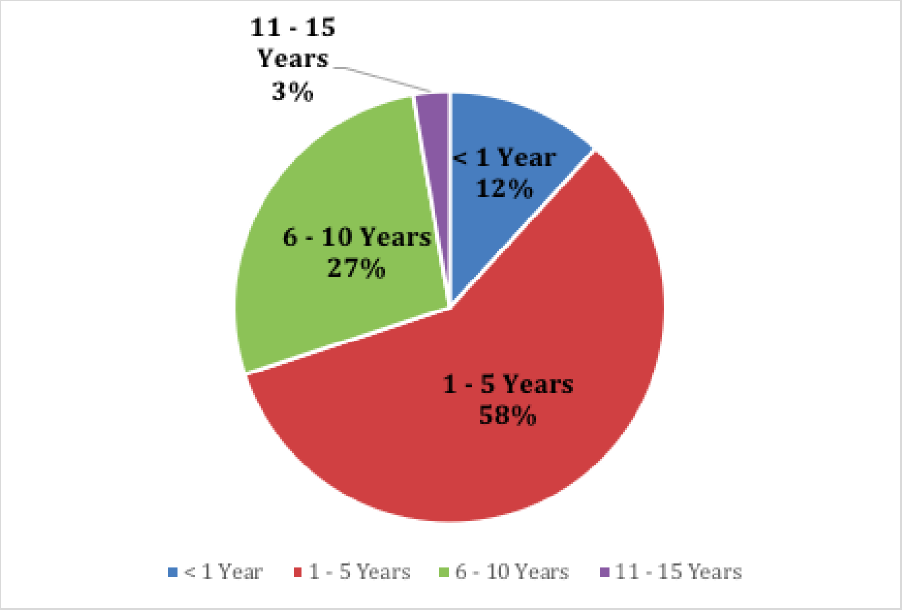


Figure 4.1: Respondents Years of Experience in E-Banking Security

Figure 4.1 indicates that majority of the respondents had between 1 to 5 years of experience in e-banking security (58.2%). This was followed by bankers with 6-10 years of experience (27.3%). There were 11.8% of bank staff with less than one year and only 2.7% of the respondents had 11 years or more of experience. The specific frequencies for each of the categories are detailed in the table below.

Table 4.3: Survey Respondents Experience in E-Banking Security

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	'1-5	64	58.2	58.2	58.2
	'11-15	3	2.7	2.7	60.9
	'6-10	30	27.3	27.3	88.2
	Less than 1	13	11.8	11.8	100.0
	Total	110	100.0	100.0	

4.5.2.1 General Characteristics of Respondents

Majority of the respondents had between 1 - 5 years of working with e-banking security. Notably there were only 3 respondents that had over 10 years of e-banking security experience. Further analysis on the characteristics of respondents are covered within this chapter.

4.5.2.2 Missing Values

Missing values can be an indicator of the respondent facing difficulties in answering questions or because the respondent deliberately left the answer blank. Analysis of the descriptive statistics on SPSS exposed missing data from one of the respondents. There was only one found and it related to the gender of the respondent. Hair *et al.* (2006) recommended that if a survey response has more than 10% of the response missing, that response should be excluded. It has been widely mentioned that a missing data rate of 5% is inconsequential whilst missing values of up to 10% are likely to introduce bias (Dong and Peng, 2013). Given that the missing response amounted to less than 1% of the responses, the researcher decided to ignore the missing data for the purposes of the gender analysis only. Overall, missing data was very low and therefore any potential for bias was kept to a minimum.

4.5.2.3 Parametric vs Non-Parametric Tests

Parametric tests assume that data is normally distributed whereas non-parametric tests do not. Non-parametric tests are ideal for ranked scales or in the event where the conditions for parametric data have not been met (Pallant, 2013). For this research, analysis revealed that the data did not meet the assumptions of parametric data. Specifically, the tests for normalisation rejected the hypothesis that the data was normal. Appendix D of this thesis shows the extract from the quantitative tests in SPSS used to assess normality. However, assumptions associated with non-parametric data were met and the researcher decided to proceed with primarily non-parametric analysis.

4.5.2.4 Outliers

Outliers can be defined as results that are highly inconsistent with the main body of the data (Fukuda and Ohashi, 1997). It has been reported that it is unclear on what effect outliers can have on an analysis (Tabachnick and Fidel, 2001). However, given that there was a chance that this could distort or impact some of the analysis, SPSS was used to help detect outliers from the survey responses. A decision was made to recode the outliers to less extreme values. The output from the SPSS analysis are attached in Appendix E of this thesis.

4.5.2.5 Non-Response Bias Analysis

Non-Response bias relates to bias which is introduced when non-respondents and respondents may have significant variances in results to survey questions. Analysis was carried out to determine whether there was non-response bias in the results received. Given the lack of data available on the non-responding bank personnel, direct comparison of those who responded and did not respond could not be carried out. An alternative option was to carry out a wave analysis to compare the difference between early and late responses (Armstrong and Overton, 1977). This is a widely used approach after a number of researchers found that non-response bias can be identified by analysing respondent data (Dalecki *et al.*, 1993; Lin and Shaeffer, 1995; Ullman and Newcomb, 1998).

The wave analysis assumes that respondents who are delayed in their response are more like those who don't respond (Zou *et al.*, 1997). To perform this analysis, the data was split into two waves of responses, separating the early and late responses for comparison. The table below outlines the mean values of the two waves:

Table 4.4: Wave Analysis to Test for Non-Response Bias from Survey

Variable	Mean: Wave 1	Mean: Wave 2	Sig.
S1	3.80	3.93	0.481
S2	3.86	3.78	0.708
S3	3.19	3.22	0.862
S4	3.38	3.68	0.085
S5	4.04	4.17	0.368
S6	3.99	4.22	0.217
S7	2.94	2.85	0.527
S8	4.32	4.27	0.571
O9	4.25	4.32	0.6
O10	4.30	4.29	0.922
O11	3.33	3.37	0.899
O12	2.72	3.10	0.087

O13	2.48	2.56	0.585
O14	4.16	4.27	0.649
O15	3.61	3.80	0.237
O16	3.22	3.17	1
O17	2.74	2.85	0.708
T18	4.12	4.20	0.7
T19	3.81	3.90	0.724
T20	4.07	4.17	0.498
T21	3.33	3.27	0.467
T22	2.59	2.61	0.943
T23	3.20	3.39	0.397
T24	4.10	3.98	0.425
T25	2.59	2.71	0.659
T26	2.23	2.17	0.727
T27	4.29	4.29	0.922
T28	3.07	3.27	0.411

The table above shows the output of the analysis carried out to estimate non-response bias. The results found that there were no statistically significant differences in means between the early and late respondents for the items in the survey questionnaire. Hence, there was no evidence to suggest that non-response bias impacted the study. The output from the SPSS analysis is attached in the Appendix F section of this thesis.

4.5.2.6 Common Method Bias Analysis

Common Method Bias relates to variance that is introduced by the measurement method rather than the constructs which the measures actually represent (Podsakov *et al.*, 2003). Harman’s one-factor analysis is commonly used to identify Common Method Bias by checking whether variance can be largely attributed to one factor (Chang *et al.*, 2010). The researcher decided to adopt this approach to test for bias due to its suitability to statistically analyse the data collected from the questionnaire. The process involved using Exploratory Factor Analysis in SPSS and required that all variables were loaded into the model. A problematic variance is indicated when all study variables produces eigenvalues suggesting that a factor accounts for more than 50% of the variance (Podsakoff & Organ, 1986). The results for this study found that the maximum variance experienced by a single factor was 11.8%. As the results indicated that the variance for a single factor was less than 50%, there was no evidence to suggest that Common Method Bias affected the survey data. The output from the analysis in SPSS is available in Appendix G of this thesis.

4.5.2.7 Factor Ratings

Due to the Likert scale being ordinal data, the primary focus of the descriptive statistics was to analyse the mean and standard deviation. Priority was given to these areas to understand the criticality for each of the variables based on the ratings from the respondents. The standard deviation helped understand the variation from the mean that the data was scored. Similar analysis has been done previously for CSF related studies such as (Teo and Ang, 1999; Shah *et al.*, 2007; Gar, 2014).

The highest rated factors were those that were rated with the highest mean and standard deviation which is less than one. Any factor that achieved a median of 2.5 or below can be seen to have relatively low criticality. The criticality ratings of each of the factors are summarised in the sections below.

Strategic Factors

The descriptive statistics for the strategic factors are given below.

Table 4.5: Strategic Factors - Descriptive Statistics

Variable	Factor	N	Mode	Mean	Std. Deviation
S8	Using historical data to determine probability of fraud during each transaction	110	4	4.3	0.643
S5	Organisation learning for fraud prevention	110	4	4.09	0.698
S6	Adaptive Policies, Procedures and Controls	110	4	4.07	0.843
S1	Timely access to information to empower management decision making	110	5	3.85	1.143
S2	Mitigation of consumer vulnerability to fraud by providing adequate Consumer Education	110	3	3.83	0.927
S4	Engaging Consultants/Specialists	110	4	3.49	0.916
S3	Awareness of Socio-Economic climate	110	4	3.2	1.065

S7	Use of specialist third parties for online transactions to enhance confidentiality.	110	3	2.91	0.991

The highest rated factors from the strategic factor category was those that were related to banks being able to adapt and make use of available information to aid the decision-making process. The respondents felt that historical data to determine probability of fraud was of the highest criticality. This indicated the importance of banks not only storing data to meet retention requirements but also using it as a tool for intelligence. In contrast, the use of third parties to secure transactions obtained the lowest mean which may suggest that respondents believed that banks should not heavily rely on external providers for securing their transactions.

Operational Factors

The descriptive statistics for the operational factors are given below.

Table 4.6: Operational Factors - Descriptive Statistics

Variable	Factor	N	Mode	Mean	Std. Deviation
O10	Financial Resources	110	3	4.3	0.841
O9	Top Management Support	110	5	4.27	0.834
O14	Strict Customer Data Protection	110	3	4.2	0.907
O15	Security Specialist Team	110	3	3.68	0.976
O11	Management and Employees Readiness to Change	110	3	3.35	0.962
O16	Strict Internal Controls	110	3	3.2	0.937
O12	Change Management	110	4	2.86	1.062
O17	Responsive Customer Service Team	110	5	2.78	1.07
O13	Regular Internal Audits in Banks	110	5	2.51	1.002

Financial resources and top management support were the highest rated operational factors. Interestingly, this does not relate to a specific measure or control that helps prevent fraud, but rather the commitment from management. It appears that the respondents take cognisance of fraud prevention being a continuous process which requires management commitment and financial resources to invest in people, technologies and processes. Customer data protection also rated highly indicating the importance of keeping customer data secure. Regular internal audits scored the lowest from the operational factor category indicating that other variables such as the internal controls that banks implement are more important than the frequency of which those controls are checked.

Technological Factors

The descriptive statistics for the technological factors are given below.

Table 4.7: Strategic Factors - Descriptive Statistics

Variable	Factor	N	Mode	Mean	Std. Deviation
T27	Authentication solutions being economically viable	110	5	4.29	0.758
T18	Using biometrics to strengthen authentication systems	110	4	4.15	0.822
T20	Using One-Time Passwords	110	4	4.11	0.77
T24	Using Artificial Intelligence to work with fraud patters and behaviours to predict, alert and prevent fraud	110	4	4.05	0.74
T19	Data Encryption	110	5	3.85	1.033
T21	Using Smart Cards for Authentication	110	3	3.31	0.751
T23	Using Multi-Layer Passwords	110	3	3.27	0.887
T28	Integration of Solutions	110	3	3.15	1.18
T25	Scalability of Security System	110	3	2.64	1.081
T22	Mixed Character Passwords	110	3	2.6	1.077
T26	User Friendliness	110	2	2.21	1.024

From table 4.7 it can be seen that variable 26, which relates to the usability and user-friendliness of systems fell into the lower values of the scale. The mode of this variable highlighted that the low criticality rating was the most commonly rated by respondents further indicating that this factor was not deemed as critical for preventing e-banking fraud.

Analysis of the standard deviation showed that the values were relatively low across the responses indicating that the data points were generally close to the mean. However, there were a few exceptions. The variables relating to Adequate Change Management, Security Specialist Team, Using Data Encryption, Scalability of the Security Systems, and Ability of Fraud Prevention solutions to integrate with other systems had higher standard deviations, indicating that the data points are spread out. The results for these variables therefore are less conclusive compared to the others.

4.5.3 Reliability Test Cronbach Alpha

Reliability can be defined as the accuracy or dependability of measurements whilst internal consistency is the degree in which items measure the same thing (Davenport *et al.*, 2015). To determine if the results achieved were justifiable using the internal consistency of the results, a Cronbach Alpha analysis was conducted. For Likert scale-based data, it is strongly recommended that the analysis uses summated scales or sub-scales rather than individual items (Gliem and Gliem, 2003). This approach was adopted and a summary of the results for each of the factor categories are given below:

Table 4.8: Cronbach Alpha Results

Category	**Cronbach's Alpha**	**No of Items**
Strategic	0.73	8
Operational	0.65	9
Technological	0.74	11

The highest rated value was for Technological factors. From the literature review phase, it became evident that most of the discussed contributory factors for fraud prevention included technology. It has been reported by Swafford *et al.* (2006) and Malhotra and Grover (1998) that a Cronbach Alpha of 0.6 and above is sufficient to be acceptable in establishing the reliability of a construct. Swafford *et al.* (2006) had also explained that generally 0.6 was the lower acceptable boundary. For this study, all categories of questions attained a Cronbach Alpha of above 0.6 and in most cases above 0.7, demonstrating internal consistency. Hence, the questionnaire obtained Cronbach Alpha values which were deemed to be acceptable in theory building studies and therefore deemed to be sufficiently reliable.

4.5.4 Bivariate Correlation

Spearman’s correlation coefficient was run to determine any correlations between the factors. This technique is a non-parametric analysis used to measure relationships between two continuous variables. Cohen’s scale was used to indicate the strength of the relationships between factors. Spearman’s correlation values (r) between .10 to .29 were deemed ‘small’, .30 to .49 were deemed ‘medium’ and .50 to 1.0 were deemed ‘large’ strength (Cohen, 1988). All factors with a correlation level (p) of 0.05 and below were deemed statistically significantly correlated. This is the common cut off point used to ascertain statistical significance (Fukuda and Ohashi, 1997). The notable correlations from the analysis are discussed below.

Strategic Factors

There was a medium strength correlation between S2 (Mitigation of consumer vulnerability to fraud by providing adequate Consumer Education) and S6 (Adaptive Policies, Procedures and Controls) which were statistically significant (r=.304, p=.001). There was also a medium strength correlation between S3 (Awareness of Socio-Economic Climate) and S4 (Engaging Consultants/Specialist) which was statistically significant (r=.317, p=.001). Although there were medium correlations between these factors, there was no clear linkage based on identified literature which the researcher could relate to.

Operational Factors

For operational factors, there were no large strength correlations. However, the following medium correlations were extracted:

1. The highest correlation was between O9 (Top Management Support) and O11 (Management & Employee Readiness to Change) which showed a medium positive correlation which was statistically significant (r=.392, p=.000). This

implied that the respondents believed that management play a critical role in preventing fraud. In addition to supporting fraud prevention activities, it implies that they should be willing to instil change within the bank.

2. O13 (Regular Internal Audits in Banks) and O16 (Strict Internal Controls) also showed a medium positive correlation which was statistically significant (r=.352, p=.000). Specifically, this related to the factor for suggesting that regular internal audits should take place to test the implementation and effectiveness of the controls. Data showed that those who rated regular internal audits with high criticality also rated strict internal controls highly. This may indicate that although internal audits should be frequent, respondents believed the controls needed to be strict in order to prevent fraud.

Technological Factors

The technological category was the only category where large strength correlations between factors were identified. The correlations can be summarized below:

1. There was a large positive correlation between T22 (Mixed Character Passwords) and T23 (Multi-Layer Passwords) which was statistically significant (r=.597, p=.000). Both measures relate to strengthening the authentication process via passwords. As passwords still remain one of the primary means of authentication, it appears that the respondents may have felt that using mixed character passwords was not sufficient to secure passwords and also felt the need for multiple layers of passwords to strengthen the authentication process.

2. There was medium positive correlation between T25 (Scalability of Security System) and T26 (User Friendliness) which was statistically significant (r=.541, p=.000). The scalability of security systems and user friendliness of systems appeared to be unrelated from literature. Therefore, the was no was no clear linkage which the researcher could relate to.

Only the strongest correlating factors for each category were discussed in this chapter. Notably, the significance level of the correlated factors mentioned above were all .000 or very close to this value, which indicates a high level of confidence in the results obtained. A table of all the correlation values have been included in the appendix of this thesis.

4.5.5 Mann-Whitney U Test: Respondent Demographics

A Mann-Whitney U Test is used to compare means of continuous variables for two different groups. This was the first analysis adopted to help understand whether the perceptions of criticality were different between stakeholder demographics. In this instance, the ratings that men and women provided for the variables were analysed. The study assumed that there was not a significant difference between criticality ratings between men and women. However, it was imperative that this assumption was tested prior to carrying out the case studies, as this could influence the target population for interviews.

Upon analysing the survey data to test whether there were any differences between the gender group of respondents, it was found that generally there was little difference between the two groups. More specifically, the output of the SPSS analysis found that out of the 28 variables tested, there was only one variable that had a statistically significant difference between the means. This is presented below:

1. The Organizational Learning for Fraud Prevention (S5) Strategic Factor survey results presented a Sig. (2-Tailed) value of 0.011.

Further details on the output of the Mann-Whitney U Test is provided in the appendix section of this thesis. Overall, only one of the factors rated had statistically significant different means. Although these factors have shown to have statistically significant mean variances between males and females, the data suggests that the differences in mean were not enough to alter the overall ratings of the factors. However, there is a potential for future studies to understand why there is a variance between gender for the factors.

4.5.6 Kruskal-Wallis Test: Respondent Demographics

The Kruskal-Wallis Test is used to analyse variances where multiple sample cases are involved (Pallant, 2013). The benefit of using the Kruskal-Wallis test as compared to the Mann-Whitney U Test is that it allows the significance of differences between more than two sample means to be tested simultaneously. This was the second analysis adopted to help understand whether the perceptions of criticality were different between stakeholder demographics. For this scenario, it was used to examine each of the factors and identify any significant variances in mean between the e-banking security experience categories.

The experience categories were coded into the following numbers rather than strings as required by SPSS. Subjects were divided into 4 groups according to their experience:

- Group 1: Less than 1 Year
- Group 2: 1 – 5 Years
- Group 3: 6 – 10 Years
- Group 4: 11 – 15 Years

The steps to analyse the subject groups involved testing the factor categories separately using the Kruskal-Wallis Test via SPSS to test if any of the factors had a Sig. value of .05 or below which meant the variances were statistically significant. For those factors that met the criteria, the ranks output table was analysed to further understand which of the groups were different. The highlights of the results have been given below.

Strategic Factors

After running the analysis, it was found that only Organizational Learning for Fraud Prevention (S5) showed significant variances between groups with a Sig. value of 0.31 between the groups. A review of the SPSS ranks output showed that respondents with ‘Less than 1 Year’ and ‘11 - 15 Year’ experience rated this factor significantly lower than the other groups.

Operational Factors

There were no significant variances between the experience groups for all the Operational Factors that were rated.

Technological Factors

The analysis revealed that User Friendliness (T26) showed significant variances between the various groups of respondents with a Sig. value of .037. The respondents with less than one years of experience gave higher ratings for the factor compared to the other categories of experience. Unlike the first scenario, this may be due to the difference in perceptions across the experience groups as all the other categories involved more experienced respondents who gave ratings which were closer together.

Given the results of the Kruskal-Wallis test, it was concluded that varying experiences in e-banking security does impact the perceived criticality of the factors. However, out of the 28 factors that were tested, only 2 of the factors have mean variances that were statistically significant. In both cases, it was noticed that the variances involved the category of respondents with less than 1-year experience of e-banking fraud.

4.5.7 Factor Analysis

4.5.7.1 Types of Factor Analysis

Factor analysis is a technique used to reduce a large number of correlated variables to a smaller number of latent dimensions (Tinsley and Tinsley, 1987). There are different types of factor analysis with the two main analysis techniques being Exploratory Factor Analysis (EFA) and Confirmatory Factor Analysis (CFA). There have been many arguments supporting the use of both Factor Analysis techniques and it is generally believed that they both have a place in research depending on the context of the study (Hurley *et al.*, 1997).

EFA is used to explore underlying factors for a set of variables, usually to discover the common factors that drive interrelationships amongst them (Swanson and Holton, 2005). It is used where researchers don't have an underlying dimension of structure before data analysis takes place. In other words, researchers can use this technique to discover the factors influencing the variables and identify which variables can go together (DeCoster, 1998). In contrast, CFA requires that the number of factors should have already been identified with the relationships between the variables and factors. The CFA is then used to test if a predetermined structure is supported by examining the expected causal connections between the variables (Hurley *et al.,* 1997). CFA is more appropriate where there is a well-developed underlying theory for the hypothesised loading patterns (Swanson and Holton, 2005).

Principal Component Analysis (PCA) is a technique that analyses data which is described by several inter-correlated variables with the goal of extracting the important information and summarising it as principal components (Abdi and Williams, 2010). It is used to translate a number of related variables into a smaller set of uncorrelated variables (Jackson, 2005). The benefit of this is that a smaller set of uncorrelated variables is easier to understand and use for further analysis than a larger set of variables (Dunterman, 1969). The PCA technique can also be used to ascertain the dimensionality of a scale (George and Mallery, 2003). Whilst some literature differentiates PCA from Factor Analysis, others such as Swanson and Holton (2005) classify PCA as a type of EFA, along with common Factor Analysis as the other alternative. They are both powerful statistical techniques that can be used for variable reduction and require large samples (10-20 per observed variable) for more stable estimates (Suhr, 2005). Joliffe and Morgan (1992) argues that PCA can be used as an alternative to common Factor Analysis and that both can provide useful insights on data.

Given that EFA is used for dimension reducing procedures whilst CFA is used for theory testing (Bryant and Yarnold, 1995), EFA was more suited for this study considering the research phase in which the survey took place. CFA was not deemed appropriate for the research phase as it is more suited to test the goodness of fit for a model that has already been defined, which was not the case at this point in the study. After considering these techniques, the researcher opted to apply PCA for this study.

4.5.7.2 Justification for Using PCA

Given that this phase of the research was still early in the study, the researcher felt the use of the PCA was more appropriate as there was a need to understand how the security measures identified could be grouped into a smaller set of factors based on their interrelationships. To achieve this, PCA was used to reduce the large set of variables into a smaller set of components or factors that summarizes the data. This is done by using the inter-correlation of the variables to form groups (Pallant, 2013). The objective was to group the factors based on statistics. The PCA technique was selected because of its preferred suitability to provide an empirical summary of the data set as compared to common Factor Analysis (Tabachnick *et al.*, 2001). Stevens (1996) also recommended the PCA technique suggesting that it is psychometrically sound and avoids some of the potential issues which occur in common Factor Analysis. The output of the PCA can be referred to as components or factors. For the purposes of this research, components were adopted as more suitable to avoid any potential confusion with the factors that had been identified during the literature review phase of this research.

4.5.7.3 Suitability of Data for PCA

Although the PCA is best suited to parametric data, it can also be used for non-parametric datasets. There have been many arguments from previous research to support this. For example, Shlens (2014) suggested that PCA is non-parametric method for extracting useful information from confusing datasets. Wilks (2006) also argued that the distribution of data need not be multivariate normal to be valid. In response to arguments that state that PCA should only be used for normal data, Jolliffe (2002, p.487) responded that "this is a rather narrow view of what PCA can do, as it is a much more widely applicable tool whose main use is descriptive rather than inferential. It can provide valuable descriptive information for a wide variety of data, whether the variables are continuous and normally distributed or not". Therefore, suggesting that PCA should not be limited to normal data only. Similarly, Mahony (2014) investigated into the use of PCA on non-normalised data and found that it is generally accepted that the normality of data is not an assumption for PCA unless there is a plan to derive further inferential data from the principal components.

There have been many studies where PCA has been applied to non-parametric data. Zali *et al.* (2011) carried out PCA and Spearman's rank correlation similar to the analysis of this study. Daszykowski *et al.* (2007) suggested that PCA can be carried out on non-parametric and recommended that outliers should be removed. Similarly, Baxter (1995) highlighted that normalised data for PCA is desirable and not mandatory. Finally, Comrie and Glenn (1998) also found that moderate departures from data normality still yielded robust PCA results. Therefore, reiterating that PCA can be applied to non-parametric data, although should be restricted to descriptive purposes.

The EBFP factors were subjected to a Principal Component Analysis (PCA) using SPSS. This is in-line with other CSF studies such as the work of Imroz (2009) where a similar methodology was adopted to reduce data to a smaller number of dimensions or factors as part of a study to identify CSF in information security risk management. Prior to performing PCA, the suitability of the data was assessed. Varimax rotation was used to determine the components for each of the factor types, The Kaiser-Meyer-Oklin (KMO) value exceeded the recommended value of .6 (Kaiser, 1974). In addition, the Barlett's Test of Sphericity reached statistical significance, hence supporting the factorability of the correlation matrix (Bartlett, 1954). The table below highlights the KMO values and the results of the analysis by factor type are discussed in the subsequent sections.

Table 4.9: PCA Suitability Assessment

Factor Category	**Kaiser-Meyer-Oklin (KMO)**	**Barlett's Test of Sphericity**	**No of Components**
Strategic	.646	.000	3
Operational	.640	.000	4
Technical	.617	.000	4

4.5.7.4 Strategic Factors

Principal components analysis revealed the presence of three components with eigenvalues exceeding 1, explaining 25.8 per cent, 19.4 per cent and 12.7 per cent of the variance respectively. Although the 3 components were suggested by the output of the SPSS, the scree plot was also analysed to identify breaks in the graph to determine the components (Cattell, 1966). Hence, scree plots were also considered in the decision on whether to retain the three components. The scree plot is shown in figure 4.2.

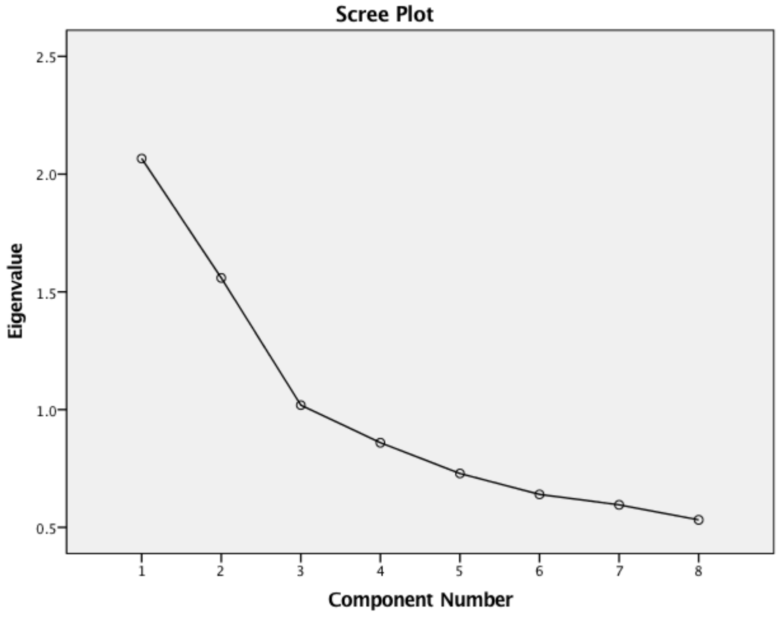


Figure 4.2: Scree Plot - Strategic Factors

To determine the appropriate number of components using the scree plot, an elbow in the graph was identified and the component number is taken to be the point at which the remaining eigenvalues are relatively small and all about the same size (Cattell, 1966). The elbow in this case starts at component three indicating that there should be 3 components. The pattern/structure coefficients that had a loading of over .3 were considered suitable for alignment to that component as recommended by (Pallant, 2013). A summary of the coefficients for each of the factors are given below.

Table 4.10: Pattern/Structure Coefficients - Strategic Factors

Rotated Component Matrix^{a}

	Component		
	1	2	3
S1	.633		

S2	.674		
S3		.715	
S4		.829	
S5	.675		
S6	.650		
S7			.852
S8			.507

The table above outlines the variables and coefficients for the components they aligned to. The components were subsequently labelled based on the factors that had been identified for each component. The components are summarised in the table below.

Table 4.11: PCA Output - Strategic Factor Groups

Component	**No of Variables**	**Critical Success Factor**	**Factor Variables**
1	4	Bank Agility via Data Driven Decision Making	• Timely access to information to empower management decision making (S1) • Mitigation of consumer vulnerability to fraud by providing adequate Consumer Education (S2) • Organisational learning for fraud prevention (S5) • Adaptive Policies, Procedures and Controls (S6)
2	2	Engagement of Subject Matter Experts (SMEs)	• Awareness of Socio Economic Environment & External Factors (S3) • Engaging Consultants & Specialists (S4)
3	2	Risk Based Controls	• Use of specialist third parties for online transactions to enhance confidentiality (S7) • Using historical data to determine probability of fraud during each transaction (S8)

4.5.7.5 Operational Factors

The PCA for the Operational Factors showed a presence of four components. An inspection of the scree plot revealed that there was a clear break after the third component. These explained 24.8 per cent, 18.6 per cent, 13.3 per cent and 9.9 per cent of the variance respectively. The output in the format of a scree plot is displayed below.

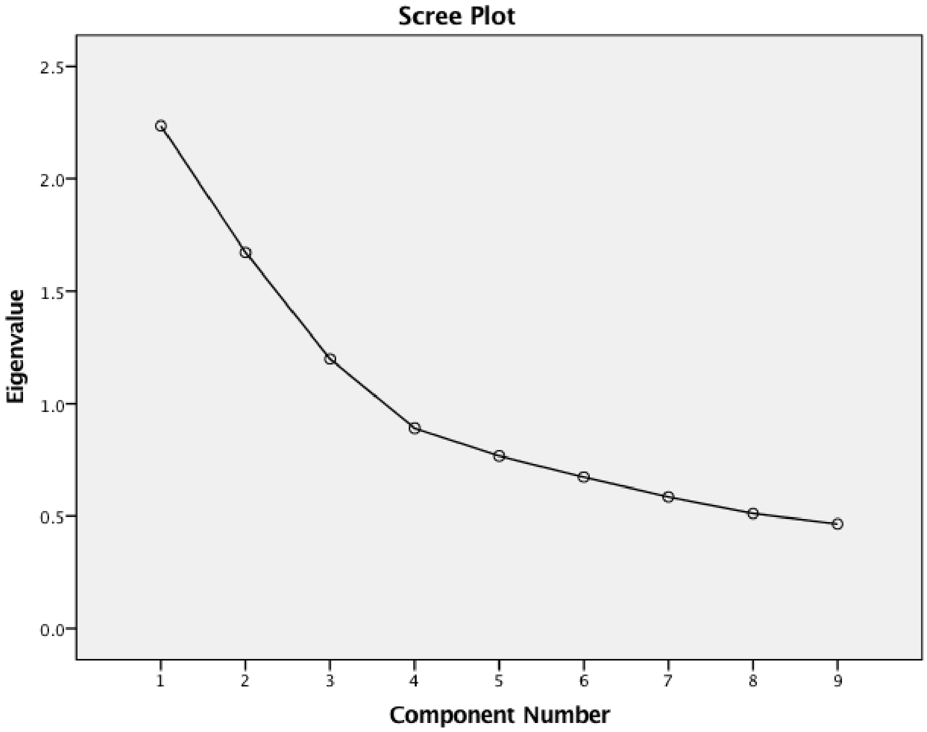
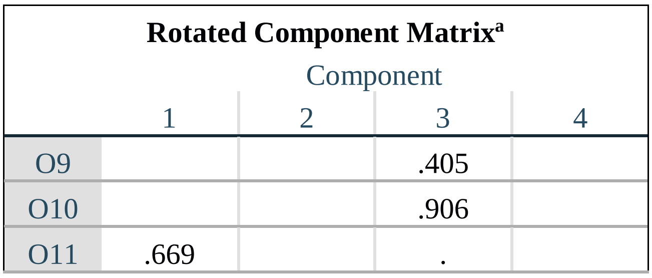


Figure 4.3: Scree Plot - Operational Factors

The dimensions of the Operational Factors were therefore reduced from 9 variables to 4 variables after the PCA was applied. The scree plot also provides a visual of the elbow which can be seen at component four. The following table provides a summary of the coefficients for each of the factors.

Table 4.12: Pattern/Structure Coefficients - Operational Factors



Rotated Component Matrix[a]

	Component			
	1	2	3	4
O9			.405	
O10			.906	
O11	.669		.	

O12	.683			
O13		.776		
O14				.873
O15		.537		
O16		.790		
O17	.725			

The table above highlights the loadings of the factors across the four components. As a result, the following operational factor components were formed.

Table 4.13: PCA Output - Operational Factor Groups

Component	**No of Variables**	**Critical Success Factor**	**Factor Variables**
1	3	Change Management & Responsive Teams	• Management & Employee Readiness to Change (O11) • Change Management (O12) • Responsive Customer Service Team (O17)
2	3	Strict Security Internal Controls	• Regular Internal Audits (O13) • Security Specialist Teams (O15) • Strict Internal Controls (O16)
3	2	Management Commitment & Support	• Top Management Support (O9) • Financial Resources (O10)
4	1	Strict Customer Data Protection	• Strict Customer Data Protection (O14)

Although the PCA output for the operational factors produced 4 components, the table above shows that the final component only had one variable assigned. Therefore, this could not be grouped and remained as a separate factor.

4.5.7.6 Technological Factors

The final PCA was conducted for the Technological factors. Results found that there were 4 components which represented 22.4, 18.0, 12.6 and 9.4% of the variance respectively. The scree plot for the Technological Factors is shown below.

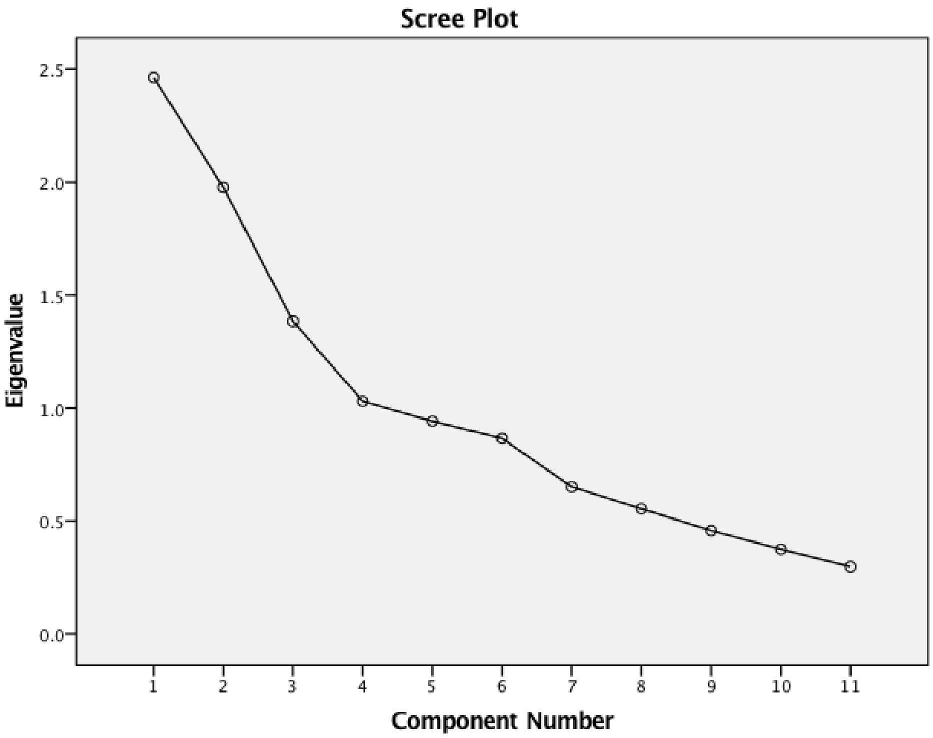
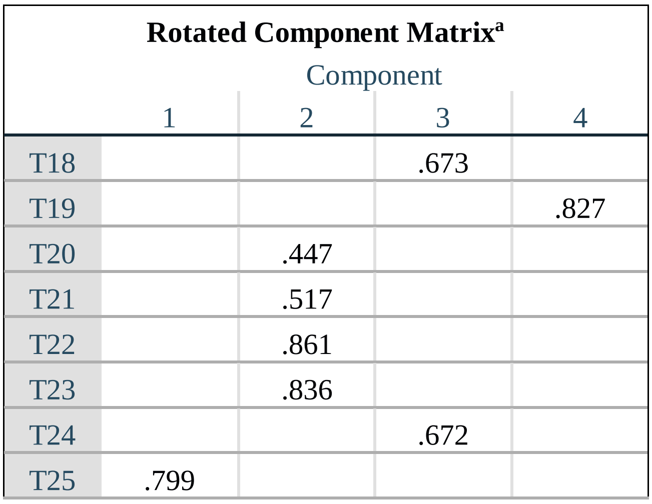


Figure 4.4: Scree Plot - Technological Factors

The dimensions of the Technological Factors were reduced from 10 variables to 4 after the PCA was applied. The scree plot also provides a visual of the elbow which can be seen at component four. The table below provides a summary of the coefficients for each of the factors.

Table 4.14: Pattern/Structure Coefficients - Technological Factors



Rotated Component Matrix[a]

	Component			
	1	2	3	4
T18			.673	
T19				.827
T20		.447		
T21		.517		
T22		.861		
T23		.836		
T24			.672	
T25	.799			

T26	.834			
T27			.637	
T28	.785			

The table above highlights the loadings of the factors across the four components. As a result, the following technological factor components were formed.

Table 4.15: PCA Output - Technological Factor Groups

Component	**No of Variables**	**Critical Success Factors**	**Factor Variables**
1	3	Usable Technology	• Scalability of Security Systems (T25) • User Friendliness (T26) • Integration of Solutions (T28)
2	4	Multi-Layer Authentication	• One-Time Passwords (T20) • Smart Cards for Authentication (T21) • Mixed Character Passwords (T22) • Multi-Layer Passwords (T23)
3	3	Biometrics & Intelligence Solutions	• Biometrics to strengthen authentication system (T18) • Artificial Intelligence to predict, alert and prevent fraud (T24) • Authentication Solutions that are economically viable (T27)
4	1	Data Encryption	• Data Encryption (T19)

Although the PCA output for the technological factors produced 4 components, the table above shows that the final component only had one variable assigned. Therefore, this could not be grouped and remained as a separate factor.

4.5.7.7 Component Validation

Given that the grouping of the components was driven primarily by the inter-correlations of the variables and the researcher’s judgement as the secondary factor, there was need to validate the output to ensure suitability. The components were therefore reviewed during the next phase of the research to ensure suitability of variable alignment to each grouping and that the components were given titles that adequately reflected the variables within each component.

4.6 New Factors introduced by Survey

Earlier in this chapter it was explained that the survey included open-ended questions to provide the respondents with the opportunity to highlight any additional factors which are critical to e-banking fraud prevention and were not captured in the previous sections. An analysis of the responses received was carried out and revealed that some of the statements were in support of existing factors whilst others suggested new factors that may be critical for preventing e-banking fraud. The table below provides a summary of the statements supporting factors which had already been identified:

Table 4.16: Statements Supporting Existing EBFP Factors

No	**Existing Factor**	**Supporting Statements**
1	Strict Internal Controls (O16)	• "Bank customers are presented with the option of activating a cheque confirmation process which adds another level of security."
2	Adaptive Policies, Procedures & Controls (S6)	• "CBN have introduced the cashless policy. This will increase tractability of transactions and serve as a deterrent to fraudsters"

The statements provided by the respondents appeared to align with some of the existing factors already highlighted earlier within the research as shown in table 4.16. Although, without further interaction with the respondent, it was difficult to reach a conclusion. In addition, there were some statements which related to additional factors that needed to be considered.

Table 4.17: Statements Introducing New EBFP Factors from Survey

No	Additional EBFP Factors Proposed by Survey Participants	Supporting Statements
1	Adoption of Europay, Visa & MasterCard platforms for Card Payments	• "EMV has made considerable impact on fraud reduction" • "EMV introduction solved menace of card skimming."
2	Stricter Controls for E-Banking Transactions	• "Stricter checks for larger amounts of money security. If activated, we are required to call the account holder to confirm they are aware of the transaction before being processed." • "The know your customer Initiative will help limit ID theft and fraud"
3	Adoption of PCI DSS for Card Data Management	• "Deployment of robust Card Management System Payment Card Industry Data Security Standard PCI DSS compliance of all parties that deal with card data"
4	Adequate Motivation of Staff	• "Adequate motivation of staff"

The table above outlines a summary of the statements submitted from the open-ended section of the survey. It introduced new factors proposed by the respondents which had not been previously covered from the literature review phase of the study, such as implementing Payment Card Industry Data Security Standards (PCI DSS). Similarly, the statement relating to the "know your customer initiative" wasn't an initiative that had been come across by the researcher, indicating the need for further understanding.

On reflection, the researcher noted that not all the factors mentioned by the respondents appeared to have the right form of a CSF. Items 1 to 3 from table 4.17 appeared to relate to adopting standards or measures to prevent fraud, which could translate into CSF. However, item 4 appeared to be of little relevance to preventing e-banking fraud. The researcher could only assume that the reference to the motivation of staff was a measure to prevent internal fraud by having more staff motivated to ensure security guidelines are adhered to. An alternative thought was that it may be related to incentivising bank staff for whistleblowing so that they report fraudulent activity, which may lead to improved fraud prevention. Given that there was limited information and details received from the open-ended question, conclusions were not formed, but rather these areas were earmarked for further investigation. Consequently, these factors were considered during the final phase of the research which involved interaction with bank staff via semi-structured interviews as part of the case study process.

4.7 Conceptual CSF-Based EBFP Framework (version 2)

The first version of the conceptual framework is presented in Chapter 2. The framework was subsequently refined based on the outcome of the survey. Not only did this phase allow the highest rated factors to be identified, but it also enabled CSF to be formed by grouping the similar interrelated variables using PCA. The revised framework is presented in figure 4.5 below:

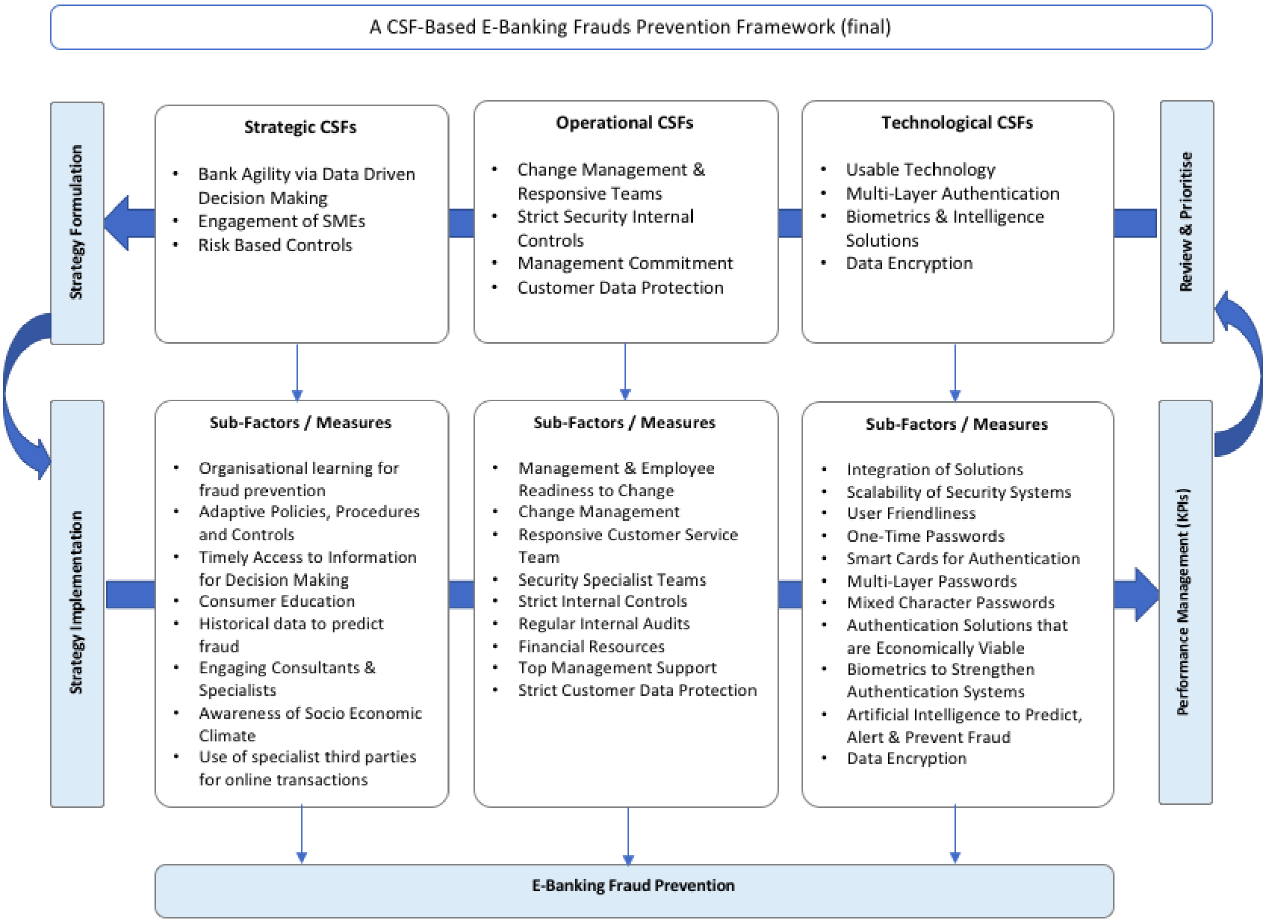

A CSF-Based E-Banking Frauds Prevention Framework (final)
Strategy Formulation
Strategic CSFs
• Bank Agility via Data Driven Decision Making
• Engagement of SMEs
• Risk Based Controls
Operational CSFs
• Change Management & Responsive Teams
• Strict Security Internal Controls
• Management Commitment
• Customer Data Protection
Technological CSFs
• Usable Technology
• Multi-Layer Authentication
• Biometrics & Intelligence Solutions
• Data Encryption
Review & Prioritise
Strategy Implementation
Sub-Factors / Measures
• Organisational learning for fraud prevention
• Adaptive Policies, Procedures and Controls
• Timely Access to Information for Decision Making
• Consumer Education
• Historical data to predict fraud
• Engaging Consultants & Specialists
• Awareness of Socio Economic Climate
• Use of specialist third parties for online transactions
Sub-Factors / Measures
• Management & Employee Readiness to Change
• Change Management
• Responsive Customer Service Team
• Security Specialist Teams
• Strict Internal Controls
• Regular Internal Audits
• Financial Resources
• Top Management Support
• Strict Customer Data Protection
Sub-Factors / Measures
• Integration of Solutions
• Scalability of Security Systems
• User Friendliness
• One-Time Passwords
• Smart Cards for Authentication
• Multi-Layer Passwords
• Mixed Character Passwords
• Authentication Solutions that are Economically Viable
• Biometrics to Strengthen Authentication Systems
• Artificial Intelligence to Predict, Alert & Prevent Fraud
• Data Encryption
Performance Management (KPIs)
E-Banking Fraud Prevention

Figure 4.5: Conceptual CSF-Based EBFP Framework (version 2)

The researcher was able to synthesis the findings after the second phase of the study and refine the framework. A total of 11 CSF was identified across the three factor categories. In addition, the variables that were aligned to the CSF were identified as sub-factors. Although this was not the final iteration, the figure depicts how the framework evolved through the first few phases of the study.

4.8 Chapter Summary

This chapter provided an insight into the survey process and the series of analysis carried out to interpret the data collected during the 2nd phase of this study. The survey was made up of profiling questions and Likert scale driven questions to rate the range of fraud prevention factors identified during the literature review phase of the research. A pilot survey allowed the survey to be tested and improved prior to it being administered. To conduct the survey, a targeted sample was approached given the need for experience-based feedback from professionals that are involved in e-banking security. The targeted population were approached via a closed web survey which bank staff were invited to take. The survey results helped identify the higher rated factors based on their criticality. After the data had been collected, there were three types of analysis that were carried out being descriptive analysis, comparisons of respondent group ratings and PCA to group interrelated factors.

Descriptive statistics were analysed to understand the profile of the respondents and rank the variables by their criticality based on their mean. The findings from the survey revealed that all but one of the factors that were identified during the literature review were rated at the higher ends of the scales on average. Furthermore, the analysis provided the opportunity to identify the factors which were rated the highest in terms of criticality. The top five factors in order of their criticality were ‘using historical data to determine the probability of fraud’, ‘availability of financial resources’, ‘authentication solutions that are economically viable’, ‘top management support’ and the use of ‘biometrics to strengthen authentication systems’.

Mann-Whitney and Kruskal-Wallis tests were used to address the following research question:

Research Question 3: Are there variations with regards to the perceptions of criticality for the factors that prevent e-banking fraud between stakeholders of different demographics?

The Mann-Whitney Test revealed that one factor had statistically significant mean variances between males and females. In addition, output from the Kruskal-Wallis test revealed that out of the 28 variables, there were 2 variables that had statistically significant differences between the respondents depending on their years of experience in e-banking security. Although this was a relatively small proportion, it did highlight the need to interact with personnel who have different levels of experience in the final phase of the research.

Finally, PCA was applied to the variables to derive a set of components. This enabled similar variables to be grouped into factors for descriptive purposes. Jolliffe (2002) mentioned that most applications of PCA successfully treat the technique as a solely a descriptive tool, and this was more pertinent for this study especially given that the data was non-parametric. The output of this analysis was a summary of factors which have been proved to be critical for e-banking fraud prevention, therefore answering the following research question:

Research Question 4: Which of the factors are the most critical in ensuring the successful prevention of e-banking fraud?

The output of the PCA can be summarised in the following diagram.

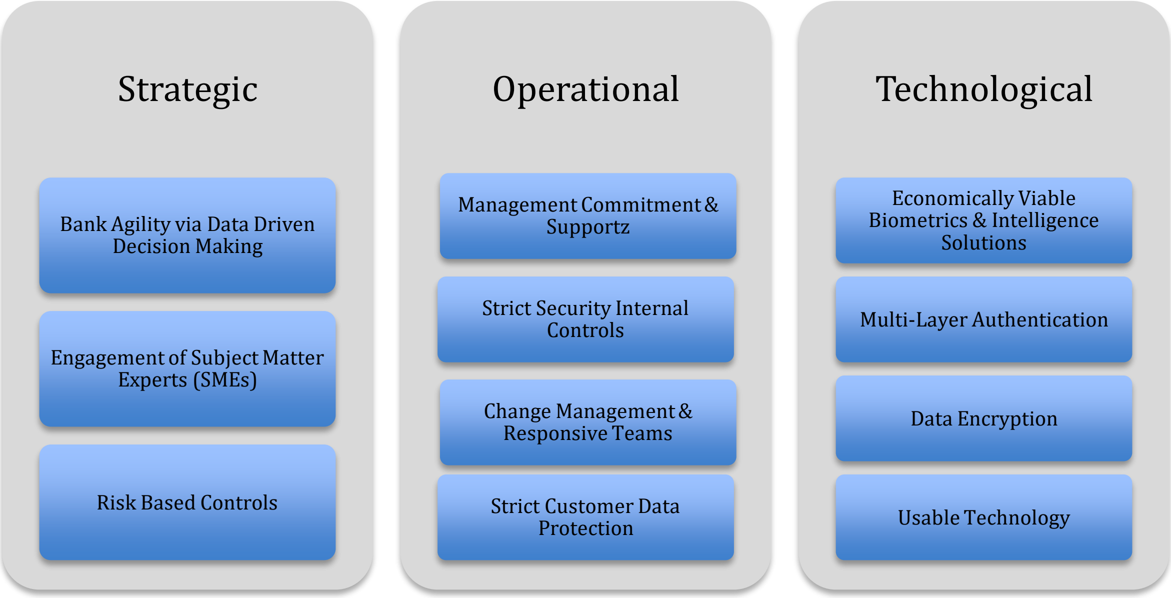

Strategic
Bank Agility via Data Driven Decision Making
Engagement of Subject Matter Experts (SMEs)
Risk Based Controls
Operational
Management Commitment & Supportz
Strict Security Internal Controls
Change Management & Responsive Teams
Strict Customer Data Protection
Technological
Economically Viable Biometrics & Intelligence Solutions
Multi-Layer Authentication
Data Encryption
Usable Technology

Figure 4.6: CSF for E-Banking Fraud Prevention

In addition to the above, the open-ended section of the survey introduced potentially 4 additional factors for further study. These were the 'Adoption of EMV platforms', 'Strict e-banking controls' such as additional levels of security based on transaction value, 'Deployment of PCI DSS for card data management' and 'Adequate motivation of staff'. These areas present room for further study as the criticality of these factors were not ascertained at this point of the study.

On reflection, the online survey administration worked well as it provided the opportunity to collect information from a large set of respondents who were spread across different states in Nigeria. Not only that, it also allowed the survey to be distributed to a targeted audience as it was imperative that feedback was obtained from people who had experience in e-banking security. From a data processing point of view, the validation defined in the survey ensured that there was minimal missing data and eliminated the need for a data entry exercise to capture the survey results.

Whilst there are many advantages in the adopted survey approach, there are also some unavoidable disadvantages which were considered. This includes the lack of opportunity to interact with the respondents to understand the rationale behind their ratings. To overcome this, the next phase of the research utilised the case study research method which involved interviews with selected staff from banks. This gave the opportunity to gain further insight into the factors and the key activities associated with each of them. The outcome of the case study is presented in the next chapter.

CHAPTER 5: CASE STUDIES

5.1 Introduction

This chapter describes the four cases that were used for this case study, which involved a representative sample of banks from the Nigerian banking industry offering similar e-banking services. In addition, the regulatory bank was also included due to its active role in the prevention of e-banking frauds in Nigeria. The purpose of this phase of the research was to develop further insights on the factors identified and rated during the previous chapters. Case studies are commonly used in research for either theory building or results validation from an earlier phase of research. For this study, it was used as the final research method as part of the methodological triangulation approach that was adopted. Semi-structured interviews were employed as the primary data collection technique and further complimented with secondary data sources such as published materials, internal memos, email messages and intranet portals.

This chapter provides a description of the cases, challenges they experienced in e-banking fraud and the banks approach to e-banking fraud prevention. The chapter discusses each of the CSF, comparing and contrasting findings from the case study. The case study seeks to further understand the CSF for EBFP and the key activities for each of the factors.

5.2 Reflective Report on the Data Collection Process

The objective of conducting the case study was to deepen the understanding on the CSF that were identified during the earlier phases of the research by understanding how the factors prevent fraud, and to validate the proposed framework. All the banks that took part of the study were notified of the objectives and what the case study would involve beforehand. In addition, they were provided with details of the issues to be discussed and assured of confidentiality in relation to any information which would be obtained during the process.

The detail of the research methodology for the case studies have been presented in chapter 3 of this thesis. Data for the case studies was collected primarily in the form of semi structured interviews, a qualitative research method. Other forms of data collection included documentation obtained from bank staff and external sources. The interviews were conducted with targeted personnel of the banks who had experience in e-banking services and its security which primarily involved staff from IT, audit, customer service and risk management. As strongly argued by the CSF theory, the staff interviewed were a combination of management and lower level staff to obtain a perspective of both levels.

Once the banks had confirmed their willingness to participate in the case study, the researcher got in contact with the bank to discuss the process and further talk through the interview requirements. In all banks, a gatekeeper was identified who served as a primary contact and assisted the researcher to identify suitable interviewees. The gatekeeper varied from bank to bank ranging from the HR department to having a focal from Managing Directors office. Although the plan was for the gatekeeper to schedule the interviews, this was not always the case and there were instances where the researcher interacted with the interviewees directly to schedule the meetings.

One of the most challenging aspects of the data collection exercise was the instances where the researcher was left to interact with the interviewees directly. In such instances, the interviewees tended to have more questions regarding the research background and delays were experienced in instances where the staff needed to discuss with their management before the interview could take place. Additionally, there had been cases where interviews were scheduled and rescheduled with relatively short notice, which the researcher had to adapt to. Although such challenges prolonged the phase of the research, this was not completely surprising to the researcher given the work ethics and demands of staff working in the banking industry.

In the letter of introduction to the banks, background of the research objectives was provided, and this was shared with the interviewees in advance. Consent was also obtained prior to carrying out the interviews and all interviewees preferred that the researcher made notes rather than them being recorded. This made the process more challenging for the researcher as there was more reliance on the notes taken and recollection of the interviews without having a recording to revert back to. During the interviews, the researcher followed the interview guide which started with an introduction to the research topic and research questions. The researcher then proceeded to ask questions in relation to the challenges experienced with e-banking fraud prevention before moving on to the main bulk of the discussion, which was on the factors for preventing e-banking fraud.

Generally, the interviews went on smoothly and the interviewees responded very willingly. As there were many topics to be covered, it was rare that an interviewee could provide details in all the areas and therefore the researcher attempted to focus on the areas that were more applicable to the interviewee's role. On occasions, the interviewees referenced documents or material that they could share with the researcher. These were usually sent after the interviews via email and in a few cases, hard copies were provided. Overall, the researcher was happy with the depth of the data collected and the banks who participated were thanked for their participation.

5.3 Case Study Bank 1 (CSB-1)

5.3.1 Background and E-Banking Services Offered

CSB 1 is a financial services provider in Nigeria. Like most banks in Nigeria, it maintains an operational base in Lagos, which is the country's commercial capital and most populous state. The bank has the vision of becoming Nigeria's retail bank of choice.

The bank is a reputable retail bank with many offices spread across the country. CSB-1 offers a broad range of e-banking services to its customers. The bank prides itself as one of the leading banks in Nigeria and emphasizes integrity as one of its core values. The diagram below provides a snapshot of the e-banking services offered by the bank.

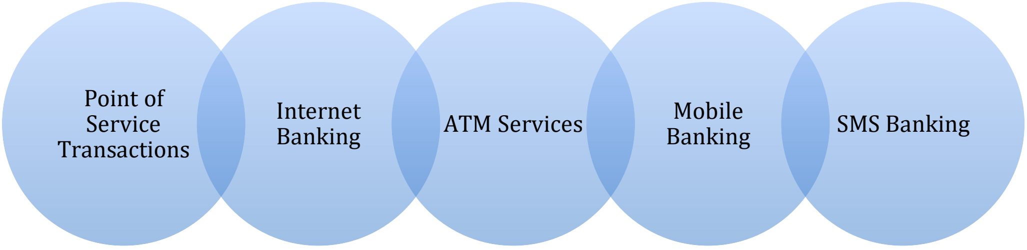


Figure 5.1: CSB-1 E-banking Services

The banks ATM's offer a range of services from withdrawing cash to purchasing airtime vouchers or the payment of bills. ATMs were the first e-banking service that the bank offered while online banking and POS electronic transactions were introduced some years later. Although the ATM was the first e-banking service that was offered by the bank, initially the machine could only be used for cash withdrawals but now the devices are used to carry out a variety of transactions. E-banking was introduced in 2011 when they started offering internet banking services. Subsequently, mobile banking, the more recent addition to their e-banking services, was introduced in 2013.

5.3.2 E-Banking Security Challenges

During interactions with CSB-1, the bank identified the following areas of where they had experienced e-banking fraud related challenges.

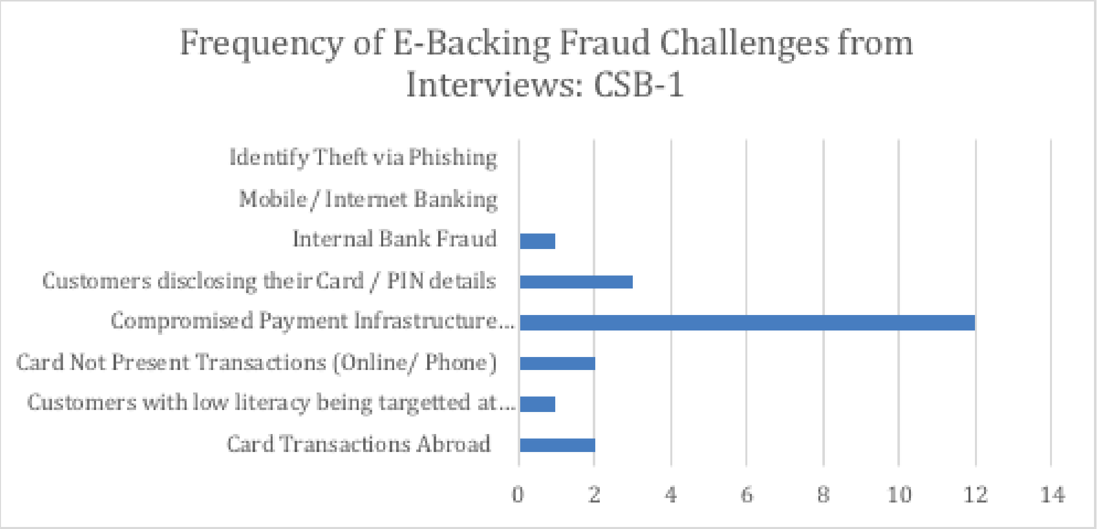


Figure 5.2: E-Banking Fraud Challenges: CSB-1

CSB-1 tends to have a lower risk appetite than some of the other banks and was less affected by e-banking fraud than some of the other commercial banks. This has resulted in the bank not being the leader in introducing e-banking services but content to be a close follower, learning from other banks and their mistakes. This was also implied by the banks ambition for a top 5 status in an extract from an Annual Statement as shown below:

“We have taken decisive steps to automate our key processes/functions within all departments in the bank in order to drive our growth and efficiency ambitions and to enable us achieve Top 5 ranking in utilization of e-business products…” - CSB-1 Annual Report, 2010

This indicated that the bank was content in becoming a top 5 bank in terms of providing e-banking services. Statistics have shown that most of the fraud incidents that arose were due to the ATMs and magnetic strip cards. Prior to the migration to the EMV platform, CSB-1 had experienced challenges with cloned cards which had been used to make fraudulent transactions.

CSB-1 stated that “There had been a series of complains relating to transactions in US and China where magnetic strip cards are still in use.” Because magnetic stripe cards could still be used to carry out transactions abroad, cards were being cloned and used even after the customers had left the country they visited. Majority the bank’s interviewees highlighted this issue. One of the interviewees lamented that this had been one of the major lapses over the years across all Nigerian banks, and not their bank alone.

One of the challenges experienced by the bank was that fraudsters were taking advantage of customers who did not know how to use ATMs. Fraudsters seize the opportunity by offering a helping hand to the customers so that they can carry out the transaction. Customers unknowingly accept and compromise their personal details, which is then later used to carry out fraudulent transactions. This aligns with the findings from Ogbuji *et al.* (2012) where it was found that banks issue ATM cards indiscriminately without considering the customers’ literacy level, leading to the customer being put at risk. It was highlighted that this was more of a potent issue in developing counties such as Nigeria.

CSB-1 stated that “Customers visiting sites that are insecure” was another challenge highlighted by the bank, which would lead to electronic fraud. CSB-1 also identified internal fraud as a challenge that had been experienced which resulted in the bank introducing stricter internal controls. One of the interviewees went as far as saying that this was their biggest risk, especially given the level of access to information that staff have. However, his views were not replicated by others.

5.3.3 Effective Security Measures Adopted

In terms of the key measures that CSB-1 takes to address the security challenges, the bank explained that a committee made up of IT, risk management, card business, audit and strategy had been setup. This committee is tasked with reviewing risks and agreeing on the best way forward. As a result, the adoption of EMV was one of the recommendations made to address the card cloning issue. The impact of this was that a risk-based approach which included a broad set of stakeholders were included. The bank reported that this approach led to a drastic decrease in fraud. This approach included being proactive by having periodic meetings to review the status of fraud and a regular forum to discuss any pressing issues. Other effective measures that CSB-1 adopted to prevent fraud included:

- Adoption of chip & pin and disabling of magnetic strip
- 2-factor authentication
- Adoption of standards such as PCI DSS, ISO 27001
- Financial and non-financial alerts to customers' mobile phones
- A variety of internal controls which include background checking of their staff
- Physical security measures such as installing anti-shoulder surfing boards
- Educating customers and staff
- Transaction limits and confirmations

"Disabling the magnetic strip fall-back option was effective as using the chip and pin features of the cards were now a requirement to transact" mentioned CSB-1. This in essence forced the added security of chip and pin upon customers. Additionally, the introduction of additional authentication measures such as SecureCode and OTPs were highlighted as key fraud prevention measures.

CSB-1 stated that EMV, PCI DSS and ISO certifications were all measures that the bank took to prevent fraud. It was explained that these measures were primarily IT driven, and their adoption was supported by consultants. The Head of Business Support added that OTPs (both hardware and software) for online banking were in use by the bank. Finally, server and database monitoring were highlighted by the bank as both preventive and detective measures. It was noted that staff were made aware of the monitoring to act as a deterrent, knowing that such monitoring and oversight was in place.

5.4 Case Study Bank 2 (CSB-2)

5.4.1 Background and E-Banking Services Offered

CSB-2 is one of many retail banks in Nigeria which is headquartered in Lagos, the countries commercial capital. Although the bank is based in Nigeria, its operations span across numerous countries. The bank has a relatively high proportion of branches and ATMs when compared to other banks. CSB-2 aims to deliver the highest standard services to its customers by being at the forefront of technology, adopting innovate e-banking services for its customers. CSB-2 offers a wide range of e-banking services similar to CSB-1.

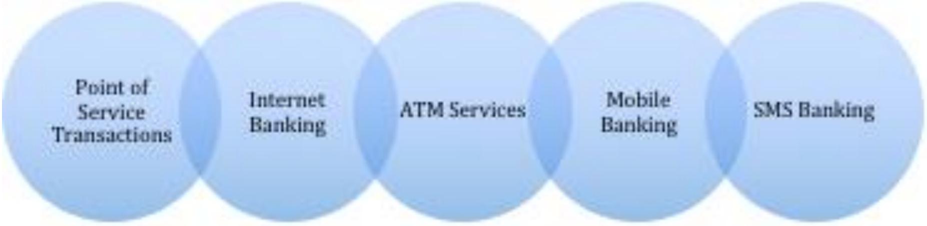


Figure 5.3: CSB-2 E-Banking Services

The bank offers a variety of e-banking services, from online banking to services via other payment providers such as QuickTeller, which allows payment of bills to be made. In addition, the bank offers mobile and SMS banking, further diversifying the channels that customers can transact from. As such, the Bank has witnessed a steady increase in Point of Service and web transactions with the figures doubling from 2015 to 2016 - CSB-2 Annual Report, 2017. CSB-2 has adopted MasterCard and Visa for its payment cards which are used for cash machines and POS offerings.

5.4.2 E-Banking Security Challenges

The figure below summarises the challenges CSB-2 experienced with e-banking fraud:

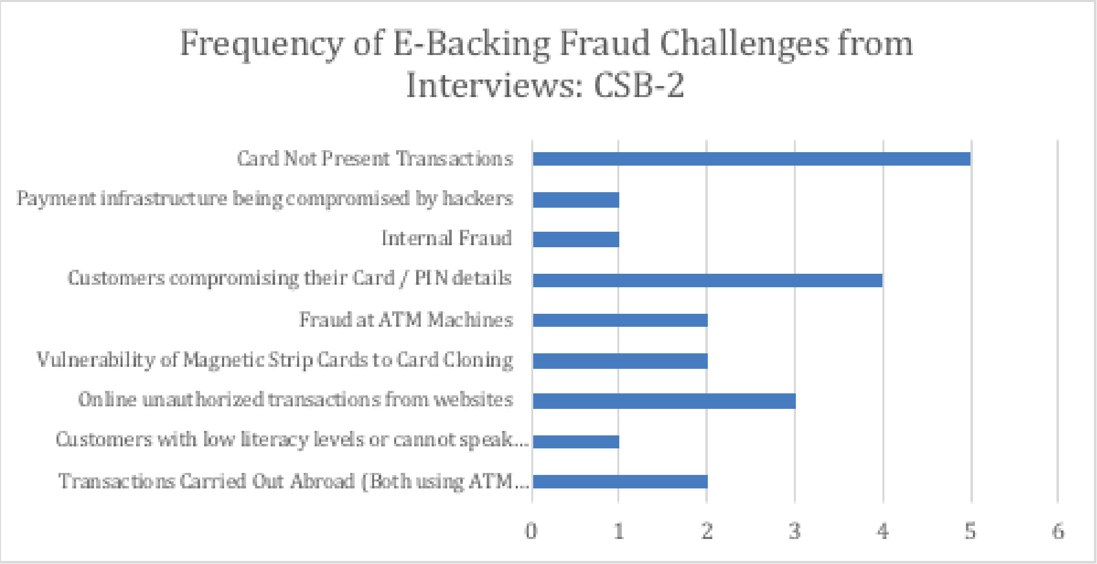


Figure 5.4: E-Banking Fraud Challenges: CSB-2

CSB-2 highlighted card not present transactions as one of their major e-banking fraud related challenges. Fraudsters were taking advantage of countries where magnetic stripe cards were still in use for payments. Cloned cards were being used to make fraudulent purchases or cash withdrawals. The US and China were some of the countries where these had been experienced from.

Another challenge identified by the bank was that customers were compromising their details. CSB-2 had received complaints from customers regarding transactions that had been carried out without the consent of the card holder. On some occasions, it was found that the card holders were sharing their card and PIN with family members so that they can transact on their behalf, usually from ATMs. This meant that the PIN was no longer secret and increased the risk of fraud by family members.

Online fraud was another area highlighted as a challenge for CSB-2. The growing number of online services being patronised by customers was understood as one of the contributory factors. Similarly, the banks appetite to give its customers a variety of payment options meant these were challenges that they needed to monitor closely and keep on top of. Globally, the challenge was that online shopping sites only required some basic card details such as the card number, expiry date, and CVV2 for transactions to be made. This made it relatively easy for fraudsters to use cloned cards.

It was emphasised that before such fraudulent activities listed above could take place, customers identity would need to be stolen or compromised. The bank highlighted that from experiences, this took place by:

- Customers compromising personal details as mentioned above.
- Scam emails which phish for customers' information, usually conveying a sense of urgency to the customer.
- Via internet cafes. Due to the lack of affordable internet services, internet cafes had been popular. Fraudsters had taken advantage of this by installing monitoring and tracking software leading to the theft of user ids and passwords.
- ATM card skimming. This involves fraudsters installing a small chip to the card reader and then stealing the customer or card information once the cardholder uses the machine. The cardholder is usually oblivious to what is really happening but rather believe there is a problem with the cash machine. It is only discovered after the details have been used for fraudulent transaction or after the bank has investigated into the matter.

In summary, the challenges primarily stemmed from customer or card data being compromised, leading to fraud.

5.4.3 Effective Security Measures Adopted

Given the banks strategy to be at the forefront offering innovative solutions while maintaining integrity, the bank takes several steps to prevent fraud.

Like CSB-1, a risk-based approach is at the heart of their fraud prevention strategy. The bank also setup a committee to govern the inherent risks that e-banking exposes the bank and its customers to. The risk management committee have the responsibility to determine the effectiveness and adequacy of the banks risk detection, measurement systems and control. The scope of this includes operational and technology risk which are the two associated with the risk of e-banking fraud.

“We carry out continuous upgrade of our card systems to ensure optimum security, absolute efficiency, cost effectiveness and customer satisfaction” - CSB-2 Annual Report,

2013. The bank therefore recognises the importance of securing their card infrastructure and data whilst offering the customers e-banking services.

Other measures the bank introduced to prevent fraud include:

- One-time passwords for authentication
- Internet banking solution to prevent phishing
- Anti-shoulder surfing boards, Anti-skimming and anti-tampering ATM devices.
- SecureCode technology for online transactions
- External Security Assessments
- Customer & staff education
- EMV and PCI DSS standards

A review of their annual reports suggests a continuous focus to fraud prevention. In 2013, the disclosed that it analyses transactions daily and produces a suspicious transactions report - CSB-2 Annual Report, 2013. The objective is for the bank to be able to identify fraudulent transactions in a timely manner. More recently in 2016, the bank outlined that its fraud risk management approach is to ensure that processes for preventing, deterring, detecting fraud, and sanctioning offenders are effective - CSB-2 Annual Report, 2016. Therefore, they have established a continuous approach to preventing fraud for their e-banking services.

5.5 Case Study Bank 3 (CSB-3)

5.5.1 Background and E-Banking Services Offered

CSB-3 is a retail bank in Nigeria. The bank has relatively less branches than many of the other banks in Nigeria and differentiates itself by offering transparent services to its customers. CSB-3 aims to be customer centric, innovative and adopt best practice.

“Employing the best people supported by technology” is a part of the banks mission - CSB-3 Annual Report, 2014. Technology is given at the backbone of the bank’s aims to be innovative and customer centric. This has enabled them to offer a wide variety of services to its customers that are comparable to the services that larger banks offer. A summary of their e-banking services is given below.

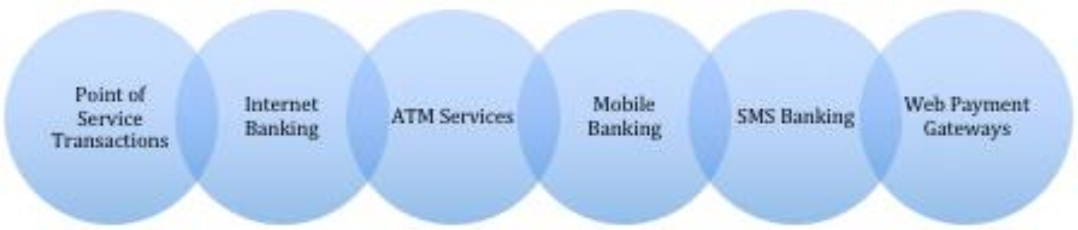


Figure 5.5: CSB-3 E-Banking Services

The bank initially started out offering ATM services only for its cards. The bank has diversified its card offerings partnering with local and global companies. CSB-3 offers POS services and more recently diversified its channels to offer SMS and mobile banking services. Overall the range of services offered are similar to both CSB-1 and CSB-2.

5.5.2 E-Banking Security Challenges

The figure below highlights the challenges in e-banking fraud experienced by CSB-3:

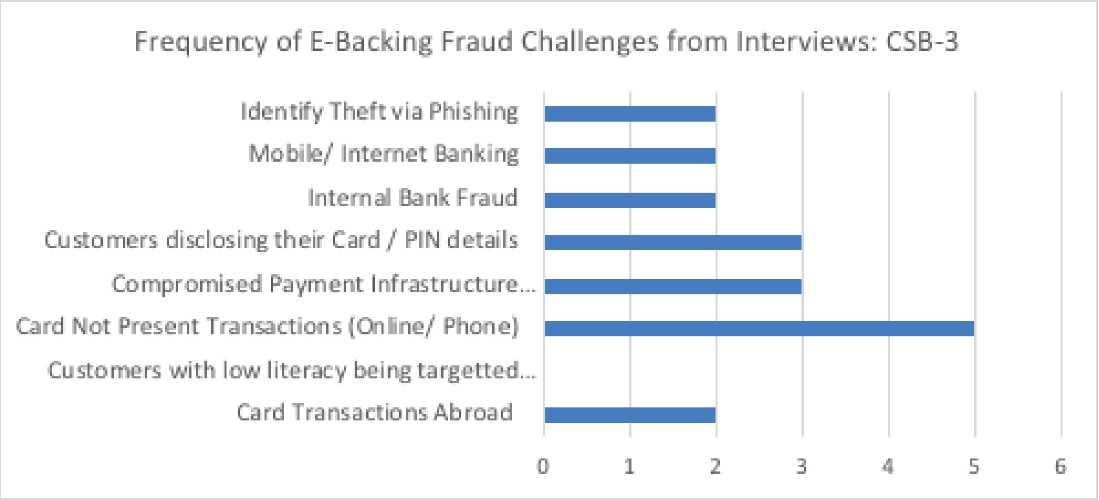


Figure 5.6: E-Banking Fraud Challenges: CSB-3

Like the other case study banks, one of the main challenges that the bank experienced involved card not present transactions and compromised payment infrastructure which leads to card cloning. Customers compromising their personal details due to carelessness was disclosed as a challenge which led to fraud over internet banking and ATM channels.

CSB-3 also highlighted that even customers who were not being careless or openly sharing their details with others could fall victim to advancing phishing methods. This could be due to email spoofing or even a lack of applying the latest security updates which can leave customers vulnerable.

5.5.3 Effective Security Measures Adopted

In terms of effective EBFP measures, the banks interviewees suggested the use of OTPs, knowledge sharing, transaction limits and adoption of security standards as effective measures for preventing fraud. Uniquely, the bank has established a process that allows them to print and share cards to customers instantly. In addition, the bank stopped printing PIN numbers but rather the customer sets up their PIN shortly after collecting their card. Both these measures are understood to be more secure and convenient for customers, aligning with the banks aim of being customer-centric.

5.6 Case Study Bank 4 (CSB-4)

5.6.1 Background and E-Banking Services Offered

CSB-4 is the regulatory bank in Nigeria. The bank is charged with administering banks and other financial institutions "with the sole aim of ensuring high standards of banking practice and financial stability through its surveillance activities, as well as the promotion of an efficient payment system" (CBN, 2015b). CBN is responsible for the issuance of operating licenses to banks and provides overall supervision on behalf of the federal government. Risk management and security play important roles in how the bank regulates e-banking services.

The bank launched a cashless economy initiative in 2012 to help transition Nigeria from being a largely cash based economy and support Nigeria's aspirations of becoming one of the top economies by the year 2020. The CBN aims at minimising the amount of physical cash in circulation and encourage electronic transactions.

"To reduce the cost of banking services (including cost of credit) and drive financial inclusion by providing more efficient transaction options and greater reach." (CBN, 2016b).

This was one of the reasons mentioned by CBN on why the policy was introduced. The policy introduced handling charges in 2012 on daily cash withdrawals for both individual and corporate bank customers, therefore encouraging customers to transact electronically.

CBN does not directly offer e-banking services to customers. However, the bank does play an important role in encouraging and regulating e-banking services. The bank also collates fraud statistics and investigates customer complaints.

5.6.2 E-Banking Security Challenges

Below is a summary of the challenges experienced highlighted during the interviews.

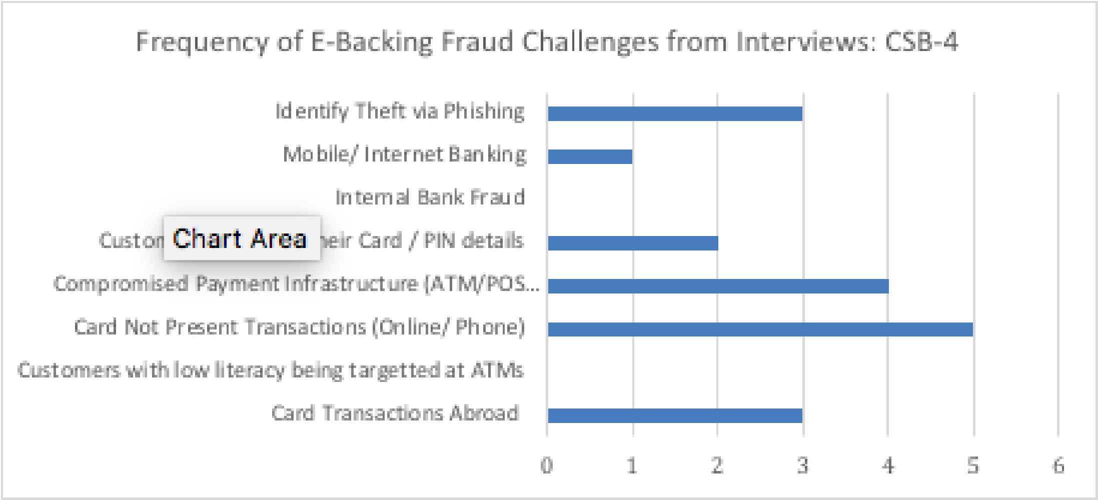


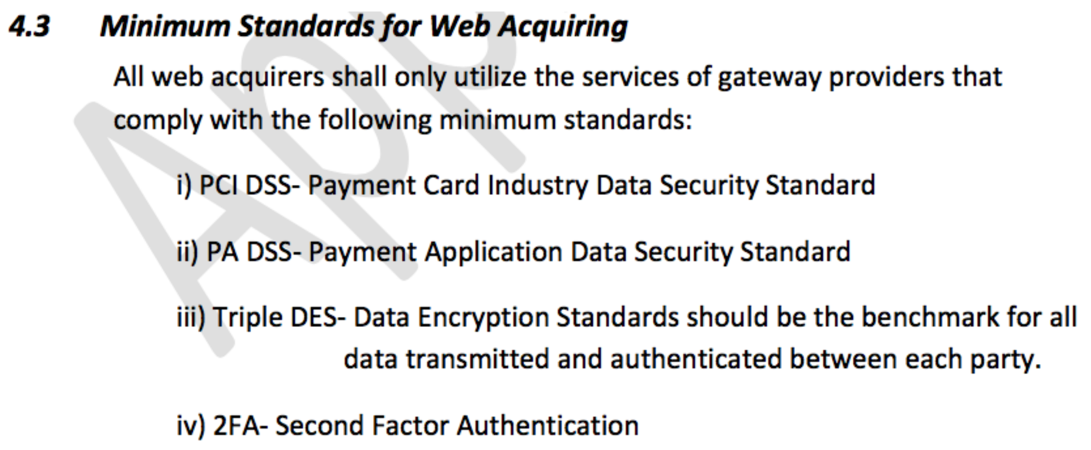
Figure 5.7: E-Banking Fraud Challenges: CSB-4

Fraud during card not present transactions was a common theme highlighted by the interviewees. In addition, fraud from card transactions abroad was another challenge experienced. Finally, tampering of ATM machines using techniques such as Lebanese loops to trap customers’ cards were also mentioned.

5.6.3 Effective Security Measures Adopted

In terms of the key achievements taken to address fraud, the regulatory bank provides guidelines for electronic payment channels which prescribes requirements in terms of security measures that banks should implement before offering e-banking services. The migration to the EMV platform was identified as a measure that has helped drastically reduce fraud. The bank continuously updates its policies to protect against changing security challenges. Circulars are released on an ad-hoc basis to direct banks on new measures that may need to be introduced, usually with deadlines for implementation.

In terms of specific measures adopted, continuous awareness and increased liabilities with banks were all suggested as effective measures taken to tackle e-banking fraud. The bank also encourages the adoption of international standards. For example, the bank has adopted standards such as Basel 3 and the International Financial Reporting Standards (IFRS). From a security perspective, the bank became the first regulatory body in Nigeria to attain certification of the ISO 27001 (CBN, 2013). The regulator also requests that the commercial banks adopt certain standard to help prevent fraud. The figure below provides an example of this.



4.3 Minimum Standards for Web Acquiring

All web acquirers shall only utilize the services of gateway providers that comply with the following minimum standards:

i) PCI DSS- Payment Card Industry Data Security Standard

ii) PA DSS- Payment Application Data Security Standard

iii) Triple DES- Data Encryption Standards should be the benchmark for all data transmitted and authenticated between each party.

iv) 2FA- Second Factor Authentication

Figure 5.8: CBN Security Standards for E-Payments (CBN, 2017)

To help address some of the challenges of fraud, the Central Bank established the Nigeria Electronic Fraud Forum (NeFF). It was explained that bank initially inaugurated an ATM fraud committee to address the menace of fraudulent transactions for card present transactions. This later evolved into the Nigeria Electronic Fraud Forum which involved the expansion of scope to fraud prevention over all electronic mediums. The audience was also expanded to include retail bank staff. The objective of the forum is to provide a platform for stakeholders to share knowledge and collectively address the challenge of securing e-banking channels. The regulator believes that no single institution can defeat fraud alone and encourages the stakeholders to work together, limit fraud and boost public confidence in e-banking services. Membership of the body includes staff of the Central

Bank, payment switching service providers, chief compliance officers and auditors of banks in Nigeria amongst others.

The following sections proceed to discuss the case study findings for each of the CSF, comparing and contrasting findings from the banks.

5.7 Case Study Findings - Strategic Factors

5.7.1 CSF 1 – Bank Agility & Data Driven Decision Making

5.7.1.1 Organisational learning for fraud prevention

Root Cause Analysis (RCA) of Incidents

To ensure that the banks learn from fraud occurrences, root cause analysis are being used. “When fraud occurs, a root cause analysis is done to understand what exactly happened. The bank then explores what could have been done to prevent it from happening again. At this point, many questions are asked and addressed, one after the other” mentioned CSB-1. CSB-2 also employs the use of causal analysis for fraud incidents identified in the Bank. CSB-2 use this as an opportunity to be abreast of the threats and vulnerabilities so that they can quickly react to minimise the risk of the bank experiencing a similar incident. The extract from CSB-2 annual report outlines the governance that the bank has introduced to oversee risks. Additionally, senior management review the controls more frequently to ensure continued effectiveness of the controls that are in place. CSB-3 ensure that all incidents are investigated with stakeholders from the audit and risk management departments. This meant that the risk team could take the learning into account for risk assessments and audit could ascertain whether it was a breach in internal controls.

Leverage local and global experience and expertise

CSB-2 claimed to have a consistent and repeatable risk assessment process which not only draws upon their experiences but also experiences externally, local and internationally. The strategy employed is to leverage knowledge from industry experts such as MasterCard, review analyst reports and engage consultants. CSB-1 and CSB-2 adopt a similar approach. CSB-3 stated that “being a relatively new bank compared to the other banks in Nigeria, the bank has been able to learn from any challenges previously experienced and deploy solutions that have proven to have worked well in the environment". Therefore, the banks did all find ways to leverage previous experiences to prevent them from experiencing some of the issues that the other banks have faced.

5.7.1.2 Adaptive Policies, Procedures and Controls

All banks' that participated in the case study adopted a risk-based approach to managing fraud, so they can be proactive. CSB-1 placed emphasis on keeping stakeholders informed and having a process that allows the bank to react speedily to any threats and vulnerabilities. An example was given on how they could effect a change to their online banking within days whilst a change to transaction limits took weeks due to the management agreement on values of the limits. Therefore, the banks agility was dependent on timely input from stakeholders. CSB-3 had a similar view where they outlined that the banks' ability to react was based on the risk involved, potential impact (financial & reputational) and the level of investment required as there are usually management approvals required to make changes which must be justified.

A risk-based approach to preventing fraud

All banks have introduced a risk management approach as their means of keeping on top of threats. CSB-1 claims that the risk management approach encourages proactive-ness which results in preventative actions taking place. The bank has adopted an enterprise risk management framework to address the various types of risks that they are exposed to such as operational risks and reputational risks. The framework runs on a platform of processes and policies that enable them to "proactively identify, measure, manage, control, monitor, and report on enterprise risk exposures" - CSB-1 Annual Report, 2012. The bank has an Enterprise Risk Management Department which reports directly to the Executive Director, Risk Management. This helps ensure that there is sufficient authority to oversee the implementation and monitoring of approved policies. An independent review of the framework by their audit division is also done on a periodic basis revalidating suitability over time.

CSB-2 introduced risk assessments that focuses on the identification and treatment of fraud related risks that the bank may be exposed to. This was the beginning of a shift in focus as the bank decided there was need to dedicate more resources to mitigate exposures given the banks strategy to offer customers payment channels that were innovative, and at times never previously been implemented in the country. The banks board through its Board Risk Committee (BRC) oversees the operational risk function in the Bank and reviews OpRisk reports on a quarterly basis - CSB-2 Annual Report, 2016. “We look at the risk exposure of all our channels and perform periodic risks assessments” stated CSB-3 also confirming that risks assessing all their e-banking channels has been operationalised.

Clearly Defined Roles & Responsibilities

In addition to the need for early visibility of risks, and support from management which are covered in separate factors, CSB-2 emphasized the need to ensure that stakeholders are not only aware of the risks, but understand the roles and responsibilities outlined by management on mitigation processes. This was because outcomes of the risk assessments would usually involve mitigation actions or initiatives that would require the support of management in the form of time, money or both. As a result, the bank setup a fraud prevention committee to help manage this. The committee is involved in understanding risks, identifying suitable controls and specific solutions to be implemented, and then overseeing its implementation. The committee is made up of Risk, IT, and Audit staff.

Due to the dynamic nature of payment systems and security risks, the Central Bank plays an active role in updating policies and guidelines which usually require banks to make changes by specified deadlines. The bank releases instructions to the banks via circulars for them on the minimum-security requirements for electronic banking. CBN did highlight that the commercial banks are actively making efforts to prevent against fraud as failure to do so can result in them being liable to losses, sanctions and even reputational damage. Therefore, the need for agility can be borne from risks, incidents or even regulatory requirements.

5.7.1.3 Timely Access to Information to Empower Management Decision Making

Periodic e-banking fraud reporting

The banks primary sources of information relating to fraud was based on customer complaints which are channelled via email, contact centres or reported directly to branches. The complaints are then used to identify which mediums the issues are coming from, of which e-banking is one of them. CSB-1 has an approved set of reports which are expected from the business units on a periodic basis, primarily monthly. This includes details of fraud breaches and top risks internally and externally.

The frequency of reporting varied within the banks. For example, in CSB-1 the Customer Complaints team were required to share a monthly report to other areas of the business. Again CSB-2 and CSB-3 had reports that were shared primarily monthly but within the departments, some reports were being shared on a weekly basis. Both CSB-1 and CSB-2 had a requirement to share fraud related statistics to their top management on a quarterly basis. "For every fraud report, measures are immediately taken to ensure reoccurrence is forestalled" mentioned CSB-2 as they highlighted the importance of preventing similar incidents.

New policies and procedures may be introduced in response to the arising issues and complaints. CSB-1 gave an example given for this is where the bank responded to fraud occurrences by limiting the number of transactions that could take place without the customer's confirmation and set that as 1 million Nigerian Naira. This appeared to be a reactive approach to adapting policies. In contrast, changes are also carried out proactively after risk assessments which occur as frequently as monthly based on the risk rating. Any identified issues or changes required are not only recommended but tracked to conclusion. Importantly, the banks emphasised the need to not only review reports internally, but also external reports.

Access to Industry Insights

The e-business team in CSB-1 has the responsibility of reviewing fraud related data in the industry so that the bank can consider external threats during its risk assessment. CSB-2 mentioned that "incidents that are prevalent in local and global business environments that are external to the bank are also analysed". Therefore, the bank also placed emphasis on understanding incidents being experienced by banks externally. Fraud data is provided to the Nigerian Electronic Fraud Forum (NeFF) which is chaired by the Central Bank of

Nigeria. The forum collates fraud statistics=from each bank, aggregates the data and then shares it with all other banks, who are also members of this forum. The information provided by NeFF aims to provide insight that allows banks to be proactive. For example, if one bank experienced a series of attacks or fraudulent activities, their experiences could be shared anonymously so that others can act and not face similar issues. All banks attested to reviewing data provided by NeFF.

Fraudulent Events Tracking

A staff from E-Services in CSB-2 confirmed that they review suspicious/failed attempts on a weekly basis. This appeared to be the only bank that was tracking and reviewing this information. Various staff of CSB-1 confirmed that the bank was reliant on compliant statistics for reporting fraud and did not cover cases that were unsuccessful. Although during the interview, staff were simply asked to comment on whether they did track this information or not, two of the staff took this as an opportunity to air their views which they believed that tracking failed attempts would be useful. In addition, a staff from IT confirmed that the bank was already looking to introduce this by analysing transaction related events. CSB-3 mentioned that they had deployed a security event management tool which brought their attention to system related threats. In addition, it was explained that NIBSS, a central switching company which processes inter-bank transactions had recently introduced a fraud monitoring solution that also tracked fraudulent activities.

In addition to the above, CSB-1 & CSB-2 both send notifications to customers for specific events relating to e-banking activity. The objective is to alert the customer to activity on their account so that they are made aware prior to potentially fraudulent transactions being completed. For example, CSB-2 notifies users via email of activity such as logins and the addition of payment beneficiaries. The notifications include information on the activity, when it was conducted and what to do if they were not familiar with the activity. The benefits include alerting users to activities which may lead to fraud before it occurs and secondly limiting impact of fraudulent transactions.

Trend Analysis & Triggers

CSB-1 and CSB-3 confirmed that fraud statistics were reviewed periodically at weekly and monthly intervals. All had mentioned that more frequent or ad-hoc reporting is done based on the rates of fraud. An example of this includes when there are increasing trends of fraud or a threat which may need to be monitored closely. The Head of Customer Services confirmed that they did analysis of complaints received monthly and e-banking fraud were a part of these complaints. This was shared with other areas of the business such as the E-Business, Information Systems Audit, Enterprise Risk Management and Operations departments. The Risk Management department added that fraud statistics were collectively reviewed by management on a quarterly basis.

In contrast, some departments within CSB-2 reviewed fraud levels on daily basis. They tracked frauds which occurred and failed attempts. There were two types of analysis carried out. One was looking at trends and patterns of frauds whilst the second was analysing each of the actual cases of fraud that had happened. For frauds that did occur, the metrics that were produced were difficult to decipher in terms of what or which systems the fraud may be traced to. However, it did provide an indication if there were issues that needed to be investigated. Distribution of the reports to other areas of the business were done monthly, quarterly, at mid-year and annually.

In terms of targets, none of the banks had set quantitative targets with respect to the levels of fraud occurrences they were working towards but rather they all were working to keep it to a bare minimum. CSB-1 mentioned that "reports are compared with the industry rates to understand how well the bank is doing in comparison to its peers". Additionally, the bank monitors fraud trends and escalates to management if:

1. There has been a consistent increase in e-banking fraud for 3 months or;
2. There is a 50% or more increase in fraud from the previous month.

This highlights that the bank has set predefined criteria for escalations to management based on the levels of fraud the bank is experiencing. This then results in additional oversight and management attention which decisions are made on how to address the issue.

CSB-3 explained that they analysed and monitored fraud statistics by the various e-banking channels, down to the point of each ATM device. The ability to quickly identify where there may be card skimming devices installed was a benefit associated with this approach.

In 2013, an initiative to track e-banking fraud statistics via a portal through NIBSS as the aggregation centre was introduced. Banks are required to submit their fraud rates monthly. These submissions form the data which CBN uses to analyse with outputs being discussed further during the NeFF meetings. CBN uses the information to helps understand how well existing policies are working and identifies potential areas of improvement. The bank gave the following examples:

- Report exposed increasing fraud was in the case of the issues that were experienced with magnetic strip cards. This led to the migration to EMV from magnetic strip.
- Analysis of fraud cases indicated the growing number of credentials were being compromised due to increased phishing cases. This led to 2-factor authentication being set as a requirement for all the banks.
- Increasing reports on offshore card payment frauds, especially in non-EMV environment led to a circular being shared by the bank requesting additional measures are put in place to prevent such fraud

Therefore, CBN also analyses statistics, both locally and internationally to understand how well the banks are performing in terms of securing their channels and how the industry compares to other countries.

5.7.1.4 Consumer Education

All the banks had emphasised the importance of educating customers to prevent fraud. Prior to 2012, CSB-1 explained that they had little emphasis on educating the bank customers on security related areas. However, this changed when an education campaign was launched in 2012 and the bank has witnessed positive results since then. CSB-2 mentioned that a large proportion of the e-banking fraud they have experienced can be attributed to customers disclosing confidential information, reiterating the need to customers to be made aware of the risks

Sharing Key Messages, Continuously

The key messages were aimed at making customers aware of some of the preventative security measures that they should take to prevent themselves from being exposed to fraudsters. This was confirmed by CSB-1 as they explained that “customers too need to play their part” implying that it was not only the responsibility of the banks to prevent fraud. Additionally, they highlighted that customer education is extremely important and linked it to issues experienced where customers shared their data. CSB-2 expressed the need for education to be a continuous process.

The word table below is a summary of the key messages provided by the banks to their customers based on the interviewees and content reviewed:

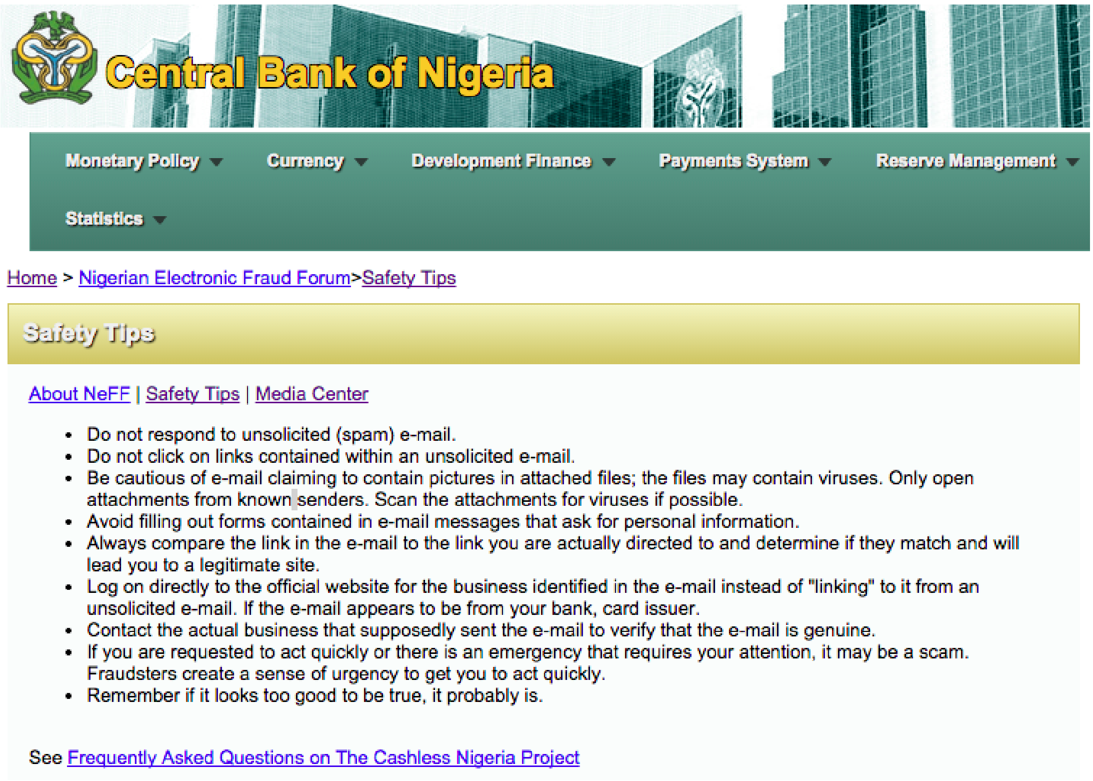
Table 5.1: Consumer Awareness Key Messages

Customer Awareness Themes	**Does the bank cover the awareness theme?**			
	CSB-1	**CSB-2**	**CSB-3**	**CSB-4**
Do not share personal information with others	Yes	Yes	Yes	Yes
Tips to guard against phishing	Yes	Yes	Yes	Yes
Only make payments through websites that have been secured via HTTPS	No	Yes	Yes	No
Reporting Lost/Stolen Cards or Fraudulent Transactions	Yes	Yes	Yes	No
Look out for shoulder surfers	Yes	No	Yes	No
Being wary of fraudsters offering assistance at ATMs to steal customers information	No	Yes	No	No
Be wary to identify if ATM may have been tampered with	Yes	Yes	No	No
Never to leave bank card out of sight	No	Yes	Yes	No
Adoption of complex passwords	Yes	No	No	No
Use anti-virus software	Yes	No	No	No
Regularly check bank statements	Yes	Yes	Yes	No

The table above shows that there are many common messages which the banks share with their customers. In contrast, CSB-1 goes into details of encouraging customers to use complex passwords such as including a combination of lower and upper-case characters in their passwords. None of the other banks appeared to cover this. This may be due to them being able to enforce such requirements, making it mandatory for customers anyway.

Although all banks highlighted the importance of customers not sharing their personal information, CSB-2 placed added emphasis on customers not sharing their personal information with family members. The bank also felt the need to warn customers to be wary of people who offer help at the ATM devices. It was explained that at times fraudsters target people who had relatively low literacy rate or not familiar with how to operate the machines to steal their information. CSB-3 believe that educating their customers is necessary to ensure the customers are aware of their duties in preventing e-banking fraud to ensure they don't become a victim of fraud. The bank mentioned that "Security is a joint responsibility for banks and customers". Hence, aligning closely with the views of CSB-1.

The interviews revealed that CBN encourages banks to educate its customers on how to prevent fraud rather than the regulator being involved. In addition, their operational guidelines for e-banking services requires banks to also educate its merchants on security measures required for mobile point of service devices. Interestingly, there was no reference to banks being required to carry out awareness campaigns to its customers, indicating that banks may be investing heavily on awareness campaigns off their own accord, acknowledging its importance. Notwithstanding, the regulator also engages in providing some safety tips to the public.



Home > Nigerian Electronic Fraud Forum>Safety Tips

Safety Tips

About NeFF | Safety Tips | Media Center

- Do not respond to unsolicited (spam) e-mail.
- Do not click on links contained within an unsolicited e-mail.
- Be cautious of e-mail claiming to contain pictures in attached files; the files may contain viruses. Only open attachments from known senders. Scan the attachments for viruses if possible.
- Avoid filling out forms contained in e-mail messages that ask for personal information.
- Always compare the link in the e-mail to the link you are actually directed to and determine if they match and will lead you to a legitimate site.
- Log on directly to the official website for the business identified in the e-mail instead of "linking" to it from an unsolicited e-mail. If the e-mail appears to be from your bank, card issuer.
- Contact the actual business that supposedly sent the e-mail to verify that the e-mail is genuine.
- If you are requested to act quickly or there is an emergency that requires your attention, it may be a scam. Fraudsters create a sense of urgency to get you to act quickly.
- Remember if it looks too good to be true, it probably is.

See Frequently Asked Questions on The Cashless Nigeria Project

Figure 5.9: Safety Tips - Website Extract from the Central Bank of Nigeria (CBN, 2015a)

The image shows an extract from the bank’s website offering some tips on how to stay safe (CBN, 2015a). In comparison to the messages that the other banks share, the messages are very similar. However, in terms of scope, the guidance from the regulator was predominantly focussed on how to guard against phishing, aligning with one of the main issues which lead to e-banking fraud as highlighted during the interviews.

Reaching Consumers Through Multiple Channels

In terms of how the bank customers are educated, CSB-1 emphasised that “the bank has introduced awareness campaigns to ensure customers also play their part in preventing fraud”. The bank communicates security tips when giving a new card to the customers but also sends emails to customers informing them of possible threats. An example of this came from the Head of Customer services when she mentioned that the bank informed their customers that the bank will never ask for their pin. Although, this could have been a proactive measure, this was likely in response to fraudulent phishing mails. The bank also conveys messages via ATMs, Emails, Text Messages and phone lines. Table 5.2 provides a comparison of the channels which the banks employ to educate its consumers:

Table 5.2: Security Awareness Channels Adopted by Banks

Customer Awareness Channel Themes	**Does the bank cover this theme?**			
	CSB-1	**CSB-2**	**CSB-3**	**CSB-4**
ATM	Yes	Yes	Yes	N/A
Emails	Yes	Yes	Yes	N/A
Magazines / Newspapers	Yes	Yes	Yes	No
Telephone (During interaction with customer services)	Yes	Yes	No	N/A
Bank Statements	Yes	No	No	N/A
Corporate Website & Internet Banking Sites	Yes	Yes	No	Yes
Social Media	Yes	Yes	No	No
Videos	No	Yes	No	No
Text Messages	Yes	Yes	Yes	N/A
Over the Counter	No	Yes	No	N/A
Flyers	No	Yes	No	N/A

Both CSB-1 and CSB-2 utilised social media to share security related messages and media with their customers. in 2014, CSB-2 attributed most complaints to a lack of awareness from the customer. The bank decided to further diversify the mediums used for their awareness campaigns which included their website, call centres, text messages, emails, videos, newspapers, flyers in the banking hall and even over the counter. CSB-3 leverage similar mediums but utilising the least number of channels. Tips were included for security on their internet banking landing page.

Educating Bank Employees

In CSB-1, a staff from Information Risk Management team in CSB-1 mentioned that "the bank makes a lot of effort to educate its personnel, especially in the field of social engineering". The bank shares tips and advice on its portal in a bid to prevent internal fraud. It was explained that staff are made aware of the consequences of internal fraud and are also encouraged to make use of the banks anonymous whistle blowing process whenever they suspect foul play. The bank also recognizes that disgruntled employees are a risk and educate its staff to be more cautious with such employees.

CSB-2 explained that “it has training workshops specifically for educating its staff”. The bank also continuously shares information within the different departments via group email accounts. For example, a single email account was available for all heads of operations from the different branches which could be used to quickly disseminate information to management at all the branches. The bank also utilized their intranet to carry out awareness campaigns. Additionally, all staff are required to complete a training take assessments on modules twice a year, separate workshops were held for merchants and consultants were required to ensure their staff are aware and adhere to security agreements.

CSB-3 has staff have awareness sessions at least once a year. The CSO confirmed that this is not restricted to fraud prevention, but information security in general. “The training covers physical and electronic security, acceptable use of technology, threats, policies and procedures, virus’s, trojans and malware etc.” In addition, he explained that their intranet contains their policies and popups are used to remind their staff. Notice boards was another medium used to share awareness messages. To confirm that the staff did understand the banks policies, they introduced annual assessments. Therefore, the banks emphasised the importance of building awareness for employees but also assessing them to confirm their understanding.

5.7.2 CSF 2 – Engagement of Subject Matter Experts

5.7.2.1 Engaging Consultants & Specialists

The banks all seek to adopt global standards relating to security. A common theme was to work with consultants and partners to proactively understand challenges and insights on fraud prevention. All the banks highlighted that they had employed the expertise of consultants to implement PCI DSS and EMV. “They have experience and come with their checklists and advice on those requirements that need to be addressed” stated CSB-3. CSB-1 mentioned that “consultants are mainly used for IT driven projects” and explained that the bank used consultants for technology related controls or standards such as EMV, PCI DSS and ISO 27001. For example, the ISO 27001 certification was achieved by employing consultants to guide the bank in implementing the security standard. The bank also used consultants for implementing PCI DSS for protecting cardholder data. Both require specialist skills or expertise and the bank decided on employing consultants with these skills to do so in conjunction with the staff of the bank. CSB-2 explained that “the body has a list of accredited consultants who they trust and work with and that banks are required to work with one of the accredited consultants to attain certification”. Therefore, although in many cases the banks chose to work with consults, there were times where it was a requirement for certification.

Independent Assessments & Guidance

Consultants were used specifically to carry out gap analysis, create a plan of activities that needed to be complete prior to certification. They would then work with the bank to setup a project team and implement the agreed plan. This would also include activities to ascertain the effectiveness of the IT security such as penetration testing. CSB-1 did highlight that once the bank had obtained the certification, it was able to maintain the controls themselves. CSB-3 used consultants for their PCI DSS implementation and explained that “it had so many sub requirements for each requirement and the bank needed someone to help develop processes and procedures and advise on technology usage” In contrast. CSB-3 opted to retain consultants after the implementation of PCI DSS to ensure they would continuously achieve recertification. Using consultants and third-party solutions was generally the banks strategy given that the bank had a small sized IT team.

5.7.2.2 Awareness of Socio Economic Environment & External Factors

External factors can influence banks in various ways. For example, new technologies can support the bank to prevent fraud whilst new vulnerabilities may leave banks more exposed than they envisaged. CSB-1 explained that “fraud data is provided to the Nigerian Electronic Fraud Forum (NeFF) which is chaired by the Central Bank”. This allows fraud to be computed nationwide, analysed and then shared with the banks. It was also found that beyond the NeFF, the Central Bank plays an active role in engaging banks and keeping stakeholders informed of the state of the economy. Banks are invited to periodic policy meetings where the economy and risks are discussed. CSB-3 made references to the reports shared by NeFF and how they provide useful information for banks to consider for their fraud prevention strategy. In addition, the forum holds meetings every two months and involves the sharing of domestic incidents and knowledge.

Finally, the use of consultants, memberships with standard organisations and interactions with OEMs were identified as means for banks to be kept aware of external factors. These interactions were also encouraged by the Central Bank as it is involved in hosting conferences where such stakeholders are invited, specifically on payment systems. This provides an opportunity to discuss future direction, challenges, innovations and global best practices.

5.7.2.3 Using Historical Data to Predict Fraud

The collation and analysis of fraud statistics was recommended by all banks. In addition, complaint data must be shared with the Central Bank on a monthly basis. The banks were all keen to ensure that when fraud does occur, it doesn't happen again.

Implementing Fraud Prevention Solutions

"All interbank transactions in Nigeria are required to pass through a fraud prevention solution" stated CSB-4. Although not all the banks had deployed solutions to predict the likeliness of fraud for other transaction types, they all agreed that it was an important measure for preventing fraud. CSB-2 had implemented a solution which predicts fraud at the transaction level. Customers are informed that their transactions are subject to fraud checks prior to the transaction being completed. In terms of how the system works, an automated alert is triggered for suspicious card transactions which results in the transaction being blocked. Similarly, the bank carries out transaction monitoring as its core banking application monitors transactional data and automated alerts are generated for any transactions that appear suspicious or fall out of policies which would have been preconfigured.

CSB-3 also uses a fraud monitoring solution but highlighted that one of the drawbacks was that this was detective and not preventive. For the transactions that raise a red flag, the bank will then follow up on each transaction. It is the audit department's responsibility to carry out investigations. The account manager then interacts with the customer as required. In the instances of fraud, this is then reported to the police and the financial crimes authority. In addition, all cases of fraud must be reported to the CBN. CSB-3 also mentioned that they were "looking at real-time threat detection and monitoring tools" which was an initiative the bank believed they would benefit from.

5.7.3 CSF 3 – Risk Based Transactional Controls

5.7.3.1 Use of Specialist Third Parties for Online Transactions to Enhance Confidentiality.

All banks involved in the case study referred to using third parties for processing their transactions. The third parties had implemented fraud prevention or monitoring solutions which were utilized by the banks. However, the interviewees did point out that the primary reason for working with third parties was not to enhance confidentiality, but to utilize the expertise of specialists that process transactions on behalf of the banks. The fraud solutions that the third parties deployed was part of the benefit in doing so.

All the banks who participated in the case study have adopted the EMV standard for chip-based payments, primarily partnering with MasterCard. CSB-1 did highlight the benefits of using these specialist companies was that they do not process the transactions themselves but provide a standard for payments which includes a set of requirements which must be followed. For example, if all the security measures as recommended by MasterCard were implemented, they would assist the banks with investigating cases of fraud.

There are other benefits with working with specialists which were brought to light. Firstly, CSB-1 explained that "MasterCard have a portal in which they could be informed when customers were travelling internationally to improve security for them when they travel". Secondly, both CSB-1 and CSB-3 highlighted that third parties usually provide continuous guidance and recommendations on how to maintain a secure environment and prevent fraud.

5.8 Case Study Findings - Operational Factors

5.8.1 CSF 4 – Change Management and Responsive Teams

Management & Employee Readiness to Change

The NeFF highlights change as being the only constant for securing Nigerian payment systems and acknowledges how this has helped Nigeria build one of the most secure payment platforms in the world. All banks have been subject to fraudulent incidents in the past and have the understanding that if their electronic channels are not secure, the customers will not use them.

Top Management as Primary Drivers

CSB-1 regularly referenced the need for management to make resources available and that in majority of instances, this was needed to effect change. There was a consensus that the banks continuous ability to change was due to the involvement of management. An example was given referring to their ISO 27001 certification. Management were required to not only make finances available to fund consultants but also involved staff leaving their daily routines to work in the project team. It was reaffirmed that this would not be possible without management commitment and their understanding on the need to change.

CSB-3 adopted a strategy to appoint the Managing Director and the Executive Director of Operations "as primary drivers" in securing the bank and ensuring that fraud is prevented. This approach meant that the top management were not only briefed but directly involved in mitigating risks. It also meant that lower level staff were aware of how seriously the executives took e-banking security. As a result, by the time approvals or resources were required, the stakeholders would have already been briefed or involved in the process of understanding what risks were being mitigated.

Awareness of Risks & Potential Impact

The Head of IS Audit in CSB-1 highlighted that “to obtain management and employee readiness to change, there is need to build awareness of the risks associated with e-banking fraud”. Without this understanding, it is difficult to get the necessary buy-in to make changes proactively. An example was provided relating to how managements understanding of fraud related risk contributed towards the bank becoming one of the first banks that were ISO 27001 certified. CSB-2 explained that “fraud prevention is not a one-time event and cannot purely be done by acquiring a solution or introducing a measure. They must understand that the challenges are continuously evolving”. Therefore, suggesting that management must understand this principle. The bank also placed emphasis on “investing in training and awareness for employees”. There needs to be the foundational understanding that fraud prevention is not a one-time but rather a continuous process. “Sharing the outcome of vulnerability assessments and penetration testing is as a good means of sharing potential risks, especially reports that come from external consultants” CSB-3 stated.

5.8.1.1 Change Management

Lean Change Management Process

To ensure changes are initiated timely, CSB-1 placed emphasis on a clear line of responsibility and delegated authority. For example, if the bank required approval from top management for each of its changes, this would limit the banks’ ability to be agile and respond to changing threats and challenges. Over time, the bank has adapted to empower managers and committees to approve different categories of changes. Further details of this have been covered in the ‘Adaptive Policies and Procedures’ factor covered earlier in this section.

Banks should be able to react quickly to risks, issues or regulatory requests. Examples of scenarios where the banks have been able to achieve this were discussed during the interviews. These were as follows:

- CSB-1 needed to prioritise their migration to an EMV platform due to increasing card fraud.

- CSB-2 was required to introduce limits on transactions over their e-banking channels
- CSB-3 needed to introduce multi-tier passwords to adhere with requirements mandated by the Central Bank.

Although each of the examples are different, they all placed emphasis on having a process to implement changes on priority. Indications were that expediting such changes tend to involve exceptional approvals from top management. CSB-1 mentioned "the more support that we have from risk management and audit, the easier it is to obtain approval" suggesting that multiple departments should be involved in agreeing required changes.

5.8.1.2 Responsive Customer Service Team

Both CSB-1 and CSB-2 emphasized the importance of customers being able to contact the bank when cards are lost or misplaced. The Head of Customer Services, CSB-1 explained that "the bank has the capability to immediately cancel cards once informed". In contrast, although the focus tended to be on card payments, CSB-3 also surfaced the issue of login credentials to internet and mobile banking. Even lost phones can warrant the need to take further measures to mitigate risk. Although there is the need for banks to be able to quickly act once they had been informed, it was stressed that there is a reliance on customers to firstly inform the banks. Without that trigger, the banks are not be able to react.

CSB-2 highlighted that "there is a reliance on cardholders reporting unauthorised transactions for both card present and card not present transactions". Therefore, emphasising the need for customers to report any issues. A staff from IT systems support in CSB-2 explained that the bank does this by having dedicated numbers that customers can call to cancel their cards and seek advice. In addition, the bank has a dedicated email address for fraud related queries and complaints. Although CSB-1 and CSB-3 also had contact email addresses, this was the only bank where they had dedicated fraud contacts.

CSB-1 claimed that the customer services teams had a key role to play in preventing fraud by sharing information to other areas of the business. This is because customer services are usually one of the first departments to be aware of such issues. Any trends or new threats are shared with E-Business and the Enterprise Risk Management departments. In addition to sharing incidents internally, there is a requirement for all banks to share a summary of the complaints received to the regulator. More recently, the Central Bank has mandated that fraud desks are introduced in all banks. The objective of this was to allow banks to quickly respond to fraud threats whilst also encouraging synergy in the industry to collaborate and effectively tackle e-banking fraud.

5.8.2 CSF 5 – Strict Security Internal Controls

5.8.2.1 Security Specialists Teams

Earlier in this chapter, it was explained that there was a reliance on consultants to provide expertise to support the banks with security related projects. In addition, banks now have their own teams which are dedicated to securing their systems and data. CSB-1 confirmed that in addition to their security team, the bank has security staff within audit, information risk management who are involved in security and fraud prevention, amongst other duties. The bank did acknowledge that they do not have all the skills required due to the broad nature of IT security but accepted the need to "buy-in those skills when they are needed". For example, with the ISO 27001 certification, the bank decided there was need to develop skills in-house. However, to achieve the initial certification, consultants were utilized. The Bank sent some of its staff for the training and deployed them to work closely with the consultants. Now the bank can support the certification itself.

Penetration tests were a common area which security teams in the banks were undertaking. Although in CSB-1, these tests were being carried out by staff from the risk management department. CSB-2 and CSB-3 referenced that penetration tests were also done but carried out by external teams.

5.8.2.2 Strict Internal Controls

There was a consensus that the banks needed to continually adjust their internal controls to prevent fraud. Although the aim was to do this proactively, there were times where the banks were reactive. A staff from CSB-1 believed that "internal staff are one of the biggest risks to banks" and highlighted that "previous incidents led to adjustments in their internal controls". An example being the introduction of OTP tokens to authenticate bank staff in addition to their customers. Similarly, CSB-2 mentioned that they "use tokens for providing access to its machines, limiting access to its systems and the ability of staff logging in with other employees' credentials". Furthermore, the case study banks have adopted several other internal controls, many of which are common. Those which are common are covered below.

Limiting staff authority

Segregation of duties to ensure that no person can initiate and complete certain processes. "This applies irrespective to whether a process is manual or automated" CSB-1 stated. Authority limits have also been assigned for the tasks that bank employees can carry out. Limits that have been implemented to minimize the risk of fraud includes credit approval limits, posting of transactions, payment of cash and expense limits. All banks have restricted access to their systems. CSB-3 disclosed that "staff cannot access core banking applications on weekends without seeking approval". Hence further limiting access for even those who are authorised to access the systems during the working week.

Role Based Background Checks for Staff

The banks adopt a combination of background checks based on the role of their staff. Pre-employment checks are carried out to validate the information provided on their CV such as work experience and qualifications. Additionally, further checks may be included depending on the person's role. For example, CSB-1 explained that "there is need for the bank to recruit personnel who have undoubted trustworthiness to work in card production" before proceeding to explain that these staff are subject to more rigorous checks such as criminal convictions and cases pending against them. CSB-2 also added that the bank has overtime become much stricter with references for both their staff and customers. "Some employees are subject to police checks" the bank explained. Although the types of employees that were required to undergo the checks were not disclosed, this gave an indication that the checks were required for specific roles.

Anonymous Whistleblowing Procedure.

In-line with global best practice, the bank has established a direct channel between whistle blowers and those who have the authority to act - CSB-1 Annual Report, 2012. The bank has also established a committee responsible for independently assessing such matters. CSB-1 stated that people are “encouraged to make use of the banks anonymous whistle blowing process whenever they suspect foul play”. This suggests that the bank encourages cases to be reported even without certainty that fraud has occurred. Further analysis into the banks whistle blower policy revealed that this was the only type of incident where the bank encouraged stakeholders to report incidents where there was a level of uncertainty, categorised as “Suspected Fraud” - CSB-1 Whistleblowing Procedure, 2014. Some of the other incidents the policy targeted that may relate or lead up to e-banking fraud include “Manipulation of Bank records/data” and “Leaking of confidential or propriety information”. Examination of the other case study banks whistleblowing procedures revealed that they had introduced a variety of mediums for issues to be raised primarily involving email, telephone and forms via their websites. CSB-1 and CSB-3 also further highlighted that all submissions are treated with full confidentiality to allay any fears people reporting issues may have.

Penetration Tests

“Penetration tests have been a common means of proactively identifying risks and loopholes in the banks system” mentioned CSB-3. The bank explained that “vulnerability assessment and penetration testing was done, especially externally once or twice a year”. Similarly, CSB-1 and CSB-2 had all confirmed that they carried out such tests internally and, in some cases, also by external consultants. The scope of the tests covered both application, network and database security. The scope of CSB-2 was similar as they mentioned that “the penetration tests cover a number of areas such as the banks network layer, application layer, firewalls etc. It also tests data sniffing and attempts to hack into ATMs”. The frequency of the tests differed from one bank to another ranging from quarterly to once every 6 months. Interestingly, the researcher noted that some of the interviewees were not aware that these tests were taking place. Although it was not clear why, it may be a deliberate attempt by the banks to not compromise the scope or quality of the tests.

Risk Assessing New Products

The banks have been able to identify risks and remediate before they become issues using the risk-based approach discussed earlier. CSB-1 gave an example of when they risk assessed an in-house application which containing card data. It was found that the URL contained an IP address and the site was not secured by HTTPS either leading to a potential vulnerability to customers' data. Because of the review, the URL was secured using HTTPS and the IP address was masked prior to release. A statement from CSB-2 indicated that a similar concept was in effect. Whist discussing penetration tests, it was confirmed that the bank "carries out tests for new systems or applications before deployment". Therefore, also offering a level of risk assessment before new services are put into wider use.

Network Separation

CSB-2 has "implemented a DMZ to protect their network and systems". Similarly, CSB-3 split their networks to limit access to systems once bank staff are on the network. It was further explained that this makes it more difficult for people external to the bank such as hackers to gain unauthorised access to those systems.

Know Your Customer & Biometric Verification Initiative

The Know Your Customer initiative was brought about to ensure all banks collect the minimum amount of information required by CBN for each account. Although it was a control imposed on the banks, the banks did see this as a positive step forward. CSB-1 explained that KYC meant that each person would provide their fingerprint biometrics as part of the enrolment process. Once enrolled, the regulatory bank issued each person with a Biometric Verification Number (BVN). The individual would then use this number to tag it to all their existing bank accounts. Failure to do so results in the account being suspended. CSB-3 mentioned that "BVN will be used for account opening and will eventually be used for authentication at ATM's and at the branches…".

During interactions with CBN, it was explained that the KYC and BVN are different initiatives, and that in most cases the KYC was being referred to in the context of both KYC and BVN. It was explained that the KYC was introduced to help promote financial inclusion across the country. At the time when this was initiated, it was estimated that a staggering 46% of adult Nigerians did not have access to financial services (CBN, 2012). On the contrary, the BVN (Biometric Verification Number) aims at providing bank customers with a single number which can be used to identify them across all banks. CBN have made the BVN mandatory for all existing and new bank customers. It is part of measures expected of all countries to put in place to combat money laundering and combating of financing of terrorism

Although the BVN initiative was relatively still new at the time of interviews, the expectation was that it would provide a foundation to ensure sufficient data for account holders is available and provide the opportunity to introduce additional controls, such as biometric authentication. Since then, in 2017, CBN released the regulatory framework for BVN operations which now requires the introduction and maintenance of a watch-list for those who may have been involved in fraudulent activities. Given that fraud prevention solutions have the capabilities of utilising such lists when predicting fraud occurrences, this will present the industry in a stronger position to better utilise such technologies.

Additional internal controls deemed effective by the banks:

Although a large majority of the controls mentioned above are common, there were some unique cases which were discussed. There are highlighted below:

- **Rotation of Internal Auditors:** CSB-1 highlighted that internal auditors were rotated across the various bank branches to limit the chances of them becoming impartial by consistently auditing the same branch and staff. This was not mentioned by the other banks.
- **"Key man" Risks:** – CSB-1 mentioned that their risk department "carry out key-man risk assessments to identify any roles where they may have resources with specific skills or expertise that are niche". The bank tries as much as possible to have two of its staff capable of carrying out each of their roles
- **Staff Disengagement Risk Assessment:** CSB-3 explained that "risks can be higher when staff are leaving the bank". Therefore, they introduced measures to not only ensure that access is revoked as soon as the staff leaves, but

additional measures to mitigate other risks should carried out. This should include changing passwords for any shared IDs.

5.8.2.3 Regular Internal Audits

Audits Covering Full Scope of Controls

The banks all had dedicated internal audit departments setup to ensure staff comply with standards and processes set out by the guidelines of the bank. CSB-1 explained that "internal audits are focused on evaluating existing controls and ensuring adherence to the banks policies". The bank confirmed that they found regular audits improve the effectiveness of the controls as it increases the likeliness of identifying controls that are losing their effectiveness and ensures full coverage of the controls can be checked. Similarly, CSB-2 highlighted that "audits cannot review all the banks controls at once, so a phased approach is necessary". Additionally, CSB-1 mentioned that regular audits serve as a deterrent as bank staff know that there is a function of the business that is monitoring their activities.

Controls Quality Assessment

"Audits will only have a greater impact in fraud prevention if the bank has the right quality of controls in place" emphasised CSB-1. This shows that there is potential value of having frequent audits in banks, however there is a caveat that the controls defined in the first place must be adequate. "The output of the audit includes recommendations on improvements to the controls that the bank has implemented" mentioned CSB-2 providing a similar message with respect for the need to assess how effective the controls are and continually improving them.

Self-Assessments

All the banks also have an independent audit function. CSB-2 specifically have oversight from the board which is made up of customer representation. The bank has taken this approach to ensure that the audits are impartial, and findings are followed through to ensure there are lessons learnt. CSB-3 has an e-fraud team within the internal audit function who are responsible for investigations. In addition, the bank uses internal-assessments to evaluate the conformity and effectiveness of controls even before an audit occurs. CSB-2 are required to complete self-assessments for operational risks and takes place at minimum once a year for all their branches - CSB-2 Annual Report, 2013. Similarly, the Head of Information Systems Audit in CSB-1 confirmed that the bank also had plans to introduce a controls self-assessment program.

5.8.3 CSF 6 – Management Commitment & Support

5.8.3.1 Top Management Support

Obtain Initial Management Support

To achieve top management support CSB-2 explained that “they must understand that the challenges are continuously evolving”. The banks all stressed the need for management support and shared a variety of examples of how such support led to improvements in fraud prevention. These are summarised below:

Example 1: The Audit/Investigations manager, CSB-1 stated that from experience, it is easier to gain top management support when there are high rates of fraud. An example of when magnetic strip cards were causing high fraud rates for all banks in the country was given. As a result, the level of management support received to introduce EMV was high, and they made available the finances required for the chip and pin infrastructure. This example required management support through funding, but also to ensure changes could be made quickly

Example 2: A staff of E-Services Security in CSB-2 mentioned that “management have shown their commitment to be proactive in introducing security measures”. An example was given where the bank implementing an identity protection solution for its customers. Another example mentioned was the reliance on management to sign off on numerous trainings which came at a cost to the bank. This training reinforced the banks ethics for the whole workforce and also some staff were sent on more specialized IT security training to further strengthen security measures. Carrying out such proactive measures would not be possible without the commitment from management.

Example 3: Head of E-Business Development in CSB-3 explained how the management supported an investment in their card management and distribution process. Bank cards are printed instantly and distributed to the customers. This limits the risk of fraud as the card details are immediately handed over to the customer where they are then required to setup a pin number by going directly to the ATM machines. The bank adopted this to minimize the risk of card or card data theft internally. An added benefit is that customers can receive their cards immediately after opening their accounts.

Establish Regular Forums with Top Management to Maintain Support

The examples mentioned above showcase how management support led to the banks investing in activities to prevent fraud. However, there appeared to be a secondary element of ensuring that management support is maintained. The Head of Compliance, CSB-3 mentioned that management can become comfortable and less concerned with fraud prevention when there have been no major series of breaches for some time. However, he pointed out that this does not necessarily mean that there are no new threats and that the situation can change very quickly. Therefore, top management support should be continuous.

CSB-2 has setup committees to ensure that e-banking fraud amongst other risk areas are given the necessary management oversight and consideration that it requires. This has been achieved by embedding it into their governance structure. In addition, the Chief Risk Officer is responsible for sharing a report quarterly to the board highlight top risks and the mitigations deployed. This is how they keep management aware and keep maintain their commitment. A staff from audit, CSB-3 stated that they ensure that management is aware of the risks involved and the importance of adopting the fraud prevention initiatives. They believed that this is an effective approach to obtaining management support by helping them understand some of the risks that the bank may be exposed to.

The banks have outlined how management support is required for financial and non-financial resources is necessary for preventing fraud. In addition, feedback has shown that although it may be easier to gain management support when there are issues, management support can also be obtained proactively, before issues arise. The risk-based approach mentioned earlier in this chapter is what banks use to bring issues to the attention of management proactively. Therefore, two common themes were identified. The first being that the banks have all established a forum which includes members of the top management team where fraud prevention issues are discussed. Secondly, management are important because of their authority to allocate resources in the form of personnel or finances.

5.8.3.2 Financial Resources

Financial resources appear to be intertwined with top management support. There were numerous references to management providing their support by approving for financial resources to be allocated to fraud prevention measures.

Cost Benefit Analysis for New Investments

A staff from the risk management team in CSB-1 highlighted although they had management commitment, this did not necessarily always translate into funds being made available for security measures and could still be challenging to get hold of. "Finances are tight and therefore thorough business cases and legwork must be carried out to ensure that the management understand the need for such an investment". Another staff added "…it is our job to ensure they are aware of the risks involved and the importance of adopting the fraud prevention initiatives". The bank went on further to mention that a cost benefit analysis is carried out to achieve this. CSB-2 similarly stated that "it is important to consider the financial cost of deployment as it affects the bottom-line but what is more important is to consider the dangers inherent in implementing sub-par systems as this could hit harder in terms of lost revenue and reputational damage". Therefore, investments required need to be fully justified to management, providing them with enough information to take a decision on whether to make the funds available or accept the risk involved of not doing so. To ensure value for money, CSB-3 mentioned that "cost is a deciding factor most of the time except if there is one solution. The bank usually goes for the cheapest option providing it meets requirements." Hence value for money is always considered.

Demonstrations & Proof of Concepts

In addition to making management aware of the risks involved in not investing in additional security measures, banks also adopted demonstrations and proof of concepts as a means of convincing management. CSB-1 elaborated that "we usually look at what's being done internationally. Sometimes its research, sometimes site visits …" stated CSB-1. Presentations and proof of concepts were also stated as some of their approaches to obtaining management buy-in so that funding is approved. Similarly, CSB-2 mentioned proof of concepts and highlighting the potential effectiveness as the approach they take to obtain finances. "We check to see what's happening in the industry. Vendors are called in to provide demos" CSB-3 explained. Thereby reiterating a similar approach to the other case study banks.

5.8.4 CSF 7 – Strict Customer Data Protection

5.8.4.1 Strict Customer Data Protection

The protection of customer data was frequently referred to during the interviews as a means of protecting customers against identity theft and unauthorized transactions. To achieve this, there were common measures that banks had adopted. Primarily, the banks adopted a combination of international security standards to safeguard their different categories of data.

5.8.4.2 Adoption of International Security Standards and Certifications

CSB-1 had made it one of their priorities to adopt global security standards and certifications to ensure their customers are well protected. The bank had certifications in ISO 27001:2013, EMV and adopted the Payment Card Industry Data Security Standard (PCI DSS) for card data. CSB-2 had adopted the PCI DSS and EMV standard for card transactions. Finally, CSB-3 had adopted ISO 27001, EMV and PCI DSS. Therefore, banks adopted a combination of security standards to help prevent fraud.

PCI DSS – Securing Card Data

CSB-1 claimed to be one of the first few banks in Nigeria to achieve the PCI DSS certification and has also since been recertified. "PCI DSS is a must and the stipulated controls are quite stringent…" mentioned CSB-1. The bank believed that the award of this certificate is an indication of the bank's commitment to securing customer information as well as maintaining a safe environment for customer transactions. The added restrictions enforced on data helped the bank limit access to data for even its own staff. One of the challenges they had previously experienced was fraudsters conniving with internal staff to unlawfully access data. The Head of Business Support believed that the measures required by PCI DSS has led to less cards being cloned and "certainly helped" the bank improve its security.

In comparison, CSB-2 also experienced a reduction in fraud after the implementation of the standard. The bank felt that the standard did greatly enhance the security of customer sensitive data. CSB-3 also felt that "the standard helped secure data not only through the transaction process but also where the data domiciles". Evidently, the banks felt that there were many benefits gained by implementing the standard. All banks engaged with consultants to help them achieve the initial certification.

EMV – Secure Customer Present Transactions

The second standard which was implemented is Europay, MasterCard & Visa (EMV). CSB-1 implemented EMV in response to the high rates of fraud that were being experienced from the magnetic strip cards. There are "cheap tools in the market that fraudsters were using" to clone cards explained the Head of Information Systems Audit, CSB-1. It was further added that EMV made it much more difficult for cards to be cloned. CSB-2 disclosed that the Central Bank of Nigeria had directed banks to migrate to EMV in 2009 after several recurring incidents of ATM fraud. However, they confirmed that were proactive and started to adopt EMV even before the Central Bank had made it a requirement. CSB-3 on the other hand did not migrate, being a relatively new bank, the bank setup their infrastructure to leverage EMV technology.

Even after the migration to the EMV platform to offer cards with chip and pin, banks were experiencing fraudulent transactions, but for transactions that took place outside of Nigeria. CSB-2 elaborated on how experiences where its card holders who travelled abroad to countries such as the US and China had experienced issues of card cloning. It was mentioned that in some cases, "a simple swipe and sign" allowed transactions to be made. To address this issue, the CBN introduced international transaction limits to cap the exposure to customers. Also, CSB-1 and CSB-2 now encourages its customers to notify the bank or MasterCard when they are going to travel. Overall, since the introduction of EMV, all banks have experienced reduced e-banking fraud rates, particularly at ATM machines.

ISO 27001 – Information Security Management System

The ISO 27001 standard was adopted by 3 of the banks. The standard specifies requirements for establishing, implementing, and maintaining information security management for organisations. It also includes requirements for a management system for the continuous assessment and treatment of information security risks to an acceptable level.

CSB-1 believes that ISO 27001 "led to the bank demonstrating high levels of data management and security processes". He explained that the bank was awarded the certificate by British Standard Institute (BSI). Keeping in-line with its determination to adopt the highest of standards, the bank later transitioned ISO 27001:2005 to the updated standard, ISO 27001:2013. CSB-3 also adopted ISO to strengthen their information security management system. The certification process took them 8 months and now carry out quarterly internal audits to ensure compliance. The bank also covers the ISO 27001 topics in their internal portal which is used for knowledge management purposes. Benefits of adopting this standard include the proactive identification of risks and implementing controls to help manage them. It also offers flexibility in adapting controls to all or selected areas of the business to protect data. The bank believes that demonstrating compliance also helps instil customer confidence.

5.9 Case Study Findings - Technological Factors

5.9.1 CSF 8 - Usable Technology

5.9.1.1 Integration of & Scalability of Security Systems

A staff from IT, CSB-1 mentioned that most enterprise solutions provide functionality to integrate with other systems directly or through middleware. Therefore, the level of emphasis involved in these areas were relatively low. In contrast, CSB-2 did mention that the integration of systems with the banks existing systems is considered although there was little indication to justify the factor being of high importance for fraud prevention.

5.9.1.2 User Friendliness

"More important than user friendliness is the security of the system being used" explained CSB-1. For example, portals should be designed to not expose more information than required, the data should be encrypted. In contrast CSB-3 did mentioned that they "go the extra mile to ensure convenience for their customers" therefore indicating that there is some level of consideration. CSB-2 did not make a direct reference to the usability of solutions but there was a reference to how biometric technology can help benefit the elderly carrying out transactions.

5.9.2 CSF 9 - Multi-Layer Authentication

5.9.2.1 One-Time Passwords (OTPs)

One-time passwords are used by all the case study banks. A combination of software and hardware driven tokens were used across the banks. CSB-1 used software tokens, CSB-2 used both software and hardware tokens whilst CSB-3 used only hardware tokens.

CSB-1 did not require OTP for all transactions. At the time of interview, the bank was using one-time passwords to authenticate financial transactions only. In contrast, CSB-2 was already using OTPs for the same purposes as CSB-1, but in addition, for adding new beneficiaries on their internet or mobile banking sites. "2 factor authentication is now compulsory, and OTP is a major part of it" CSB-2 explained. Additionally, the bank uses OTPs for accessing new menu items that had not previously been accessed by the customer. “One-time passwords are used for authenticating financial and non-financial transactions” stated CSB-3. Due to its effectiveness, both CSB-1 and CSB-3 confirmed they were looking to expand the usage of OTPs further to a broader range of their applications.

CSB-1 claimed that the reduction of fraud can be partially attributed to OTPs being one of the key measures that prevented this. Although the banks varied slightly in terms of the types of OTPs that were used, the feedback of OTP as a fraud prevention measure was very positive from all banks.

5.9.2.2 Smart Cards for Authentication

Smart cards are used by all the case study banks for their credit/debit cards. Two of the banks had migrated from magnetic stripe cards to those which utilized smart cards. In addition, the third bank was relatively new and did not adopt magnetic strip cards due to the known risks, choosing to adopt smart cards from inception. The primary benefit of this is that the technology was a more secure approach which highly reduced the chances of card cloning, addressing the issue which many of the banks had faced with magnetic strip cards. The manager of E-Business CSB-1 confirmed this by stating that “Smart card technology eliminated the risk of card cloning”.

For all the case study banks, there were several references to the EMV platforms. Further details have been provided earlier within the Strict Customer Data Protection section of this chapter.

5.9.2.3 Multi-Layer Passwords

All three retail banks involved in the case study use a minimum of 2-factor authentication as this was a requirement from the Central Bank. CSB-1 explained that “after the risk team had noticed some breaches in passwords we also introduced memorable words” adding an additional layer of password protection. CSB-2 explained that “one-time passwords have been adopted to prevent fraud on web channels for both cards and internet banking”. The bank had the most stringent set of multi-layer authentication requiring a combination of an online banking password and a one-time password (OTP) to complete transactions. For financial transactions, a memorable password was also required similar to CSB-1. Although it reduces the convenience to customers, it was highlighted as being effective as one of the layers refer to something the user has whilst the other relates to something they know, making it more difficult to breach. Additionally, for customers to process financial transactions, a third level of authentication is in place which requires the customer to enter a secret answer prior to the transaction being completed.

5.9.3 CSF 10 - Biometrics & Intelligence Solutions

5.9.3.1 Authentication Solutions that are Economically Viable

The banks all elaborated on how all security measures needed to be of value, and not solely authentication solutions. Suitability, convenience to customers, accuracy, risk and the cost are all common themes which are taken into consideration. Further details had already been captured in the financial resources section of this chapter.

5.9.3.2 Biometrics to strengthen authentication

All the case study banks were aware of the benefits of adopting biometrics. Biometrics was mainly referenced in its physiological form, specifically fingerprints. CSB-1 mentioned that "… people cannot steal each other's biometrics making identity theft more difficult". Although the bank was not using biometrics for authentication at the time, plans were being put in place to deploy biometrics. In preparation, the bank disclosed that its staff had already visited South Africa to see how it is being used by some of the banks.

CSB-2 believed that biometrics could help prevent fraud but concluded that it was not feasible at the time due to the investment in ATM terminals that the bank had already made which would need be replaced. Since then, the bank has added fingerprint authentication capability to its mobile banking application, for mobile devices that support this method of authentication. CSB-3 felt that it was a matter of time before all banks would adopt this technology. For example, the CSO recommended that fingerprint biometrics should be used in their ATM machines and at their branches.

5.9.3.3 Artificial Intelligence to predict, alert and prevent fraud

The case study clarified that this area had been covered earlier within this chapter under the section 'Using Historical Data to Predict Fraud'. There appeared to be an overlap between the factors as artificial intelligence was seen to be used for determining the logic of fraud prevention systems.

5.9.4 CSF 11 - Data Encryption

5.9.4.1 Multi-layer encryption

Data encryption was primarily referenced in the context of PCI DSS. All banks did disclose the need for data to be encrypted as a means of safeguarding information. However, the responses did not indicate that this measure was critical to preventing fraud, especially given that the challenges experienced were primarily not related to fraudsters hacking the banks systems. The Central Bank mandated that Triple DES encryption is adopted as a standard for electronic transactions. All the banks confirmed that data encryption is one of the steps taken to protect customers sensitive information.

“Any data accessible from portals should be encrypted” mentioned CSB-2. They further disclosed that multiple levels of encryption are used which spanned across their storage devices, databases and networks to protect data whilst being stored or in transit.

5.10 Outcome of CSF-Based E-Banking Frauds Prevention Framework Review

During the interviews, the opportunity was used to validate the grouping of the factors to ensure suitability and applicability. This was in accordance with CSF theory which encourages validation via professionals to utilise their experiences. Additionally, the structured-case approach acknowledges that the theory development process may require several iterations based on additional insights and knowledge that is obtained. During the review, the following suggestions were made:

Table 5.3: CSF Based Framework Suggestions for Improvement

CSF	Feedback Received
Engagement of Subject Matter Experts (SMEs)	The “Using historical data to determine probability of fraud during each transaction” factor was more suited to the third component, Risk Based Transactional Controls.
Bank Agility via Data Driven Decision Making	It was suggested that Consumer Education should be a CSF on its own due to its importance. Additionally, it was highlighted that the education was not only for customers, but also for staff, contractors, vendors and other stakeholders. The term stakeholder was deemed more encompassing.
Usable Technology	Although it was felt that these factors were necessary for banks to provide electronic services, the general responses obtained suggest that these factors were not deemed to be critical for fraud prevention.
Data Encryption	It was suggested that data encryption was one of the requirements of PCI DSS and PCA DSS which had previously been discussed. Given the challenges experienced, it was believed that this is a measure amongst many others required to meet security standards. It was felt that rather than being a CSF on its own, it should be captured within the required security standards.
Strict Data Protection	There were comments to suggest that although the protection of customer data is important, the banks other information also needed to be protected. An example was given by CSB-3 where if an internal staff had unnecessary access rights, they would be empowered to carry out unauthorised actions such as replicating users, adding additional levels of access to other which may then lead to fraud. In this respect, the customers’ data was strictly protected, but those measures would still be breached. Therefore, an Information Security Management System takes a holistic approach to protecting banks data.

Feedback from these reviews as summarised in table 5. helped instil confidence in the classifications adopted but also highlighted some of the factors that were more suited to other classifications.

5.11 New CSF from Case Study

The case study process identified two new factors, and they are discussed below:

1. Information Security

EMV and PCI DSS were factors that were identified during the survey phase of the research that required validation. In addition to these, ISO 27001 was a certification that was regularly referenced by three out of four of the banks. This certification involves implementing and maintaining an information security management system which incorporates a risk-based approach to security. In addition, it recommends several measures organisations should implement to secure their information. The interviewees believed that adopting this standard has helped strengthen their organisations security, therefore contributing to the prevention of fraud.

The case study revealed that this was just one of the security standards adopted by the banks with others being PCI DSS, PA DSS and EMV. Each of the standards all aim to increase security in different areas. For example, PCI DSS focusses on securing card data whilst PA DSS focusses on security of applications. Therefore, rather than differentiating one standard as critical for e-banking fraud prevention, the emphasis was on adopting the right combination of standards to adequately secure information through the different transaction categories. For example, EMV was discussed in the context of card present transactions whilst PCI DSS would help security of card present transactions. Essentially, banks are adopting measures to ensure information is secured for each of their channels.

2. People Awareness & Training

People have been severally identified as weak links. All case study banks highlighted the importance of building awareness to a variety of stakeholders and not only its consumers. This ranges from the banks staff, vendors, temporary staff, consultants and merchants. Although the importance of awareness and training has been emphasised previously, including previous phases of this research, the case study revealed some of the key messages that should be given. Additionally, previous literature tended to either focus on customers or staff awareness. This study has revealed that ‘people’ should be considered in the broader context. People who work for the bank, provide services on the behalf of the bank or are the end users of such services should all be identified and trained. Finally, the banks highlighted that a combination of channels should be utilised to help improve results.

5.12 Chapter Summary

This chapter has provided a summary of the case study process and a reflective summary on what had transpired during the case study exercise. Four financial organisations took part in the case studies with banks that offered a similar range of e-banking services to their customers. The data was collated in qualitative form by semi structured interviews and the review of documentation and archives available to the researcher. The data received were organised into themes and have been discussed in accordance with the categories discovered during the research process.

The case study formed the final phase of the research and provided the researcher with further insight into the issues experienced and further understanding into the factors that the banks have adopted to help prevent e-banking fraud. Importantly, the banks emphasised that fraud prevention is a continuous process that requires continuous risk management.

Themes related to all previous CSF had been discussed during the cases study with additional understanding on some of the common key activities related to the CSF. For example, with regards to the CSF on bank agility, the banks explained that they had adopted an enterprise-wide risk management approach, incorporating operational risk management procedures into their decision-making process. Also, in relation to the ‘Strict Internal Controls’ CSF, common activities such as separation of duties, employee background checks and whistle blower policies were all reported as effective in preventing fraud.

During the survey phase of the research, four factors were introduced in the open-ended questions as mentioned in the previous chapter. The case study surfaced these new factors for validation. The outcome found that EMV, PCI DSS were all confirmed to be important in the prevention of e-banking fraud and it was gathered that these along with other international security standards should be adopted to protect data. On the contrary, it became apparent that the KYC was not an important factor as this initiative was purely focussed around financial inclusion. Similarly, there was no further indication that the adequate motivation of staff was a CSF.

The case study introduced two new CSF. The first relating to the adoption of Information Security. Banks recommended the adoption of international security standards to help secure data through different transaction types offered to customers. Secondly, People Awareness & Training was identified. All banks placed emphasis on this area as historical security weaknesses have been down to compromises made by customers or their employees. The banks have found that creating awareness for all people who they engage with is as effective means of preventing e-banking fraud.

Overall, this chapter has validated previously identified CSF, provided further insights and introduced new CSF. The next chapter discusses the overall findings of the research.

CHAPTER 6: FINDINGS & EBFP FRAMEWORK

6.1 Introduction

This chapter discusses the results of the research phases in accordance with the research objectives. The previous chapters have presented the results of the survey and case study independently. This chapter discusses the results collectively whilst further referring to literature to evaluate the results.

The aim was to extend the Critical Success Factor theory applying it to e-banking services, specifically for preventing fraud in Nigeria. As defined by Wacker (1998), theory is considered to be made up of the four following components; Definitions of Terms or Variables, Domain, Set of relationships and Predications. The intension of the study was to produce an output that can be of use to both researchers and working professionals in the industry. In order to achieve this, a triangulated strategy was adopted where a combination of research methods and data sources were employed. The end product of qualitative analysis are generalisations that have been formed from peoples' experiences (Ayres *et al.*, 2003). Hence, in this research, it related to generalisations on CSF for E-Banking Fraud Prevention.

6.2 Theory Extension Process

The CSF theory was extended to the topic of e-banking fraud prevention, specifically in the context of the Nigerian Banking Industry. To achieve this, the researcher firstly examined existing CSF theory to understand the principles and qualities of CSF such as the CSF levels, types, categories, techniques for identification and its application. All these have already been outlined in the literature review chapter of this thesis. Similarly, previous CSF studies were discussed within the same chapter making it evident that the theory had not been applied in the context of this research. This not only reiterated the gap which the research set out to address but also discussed how CSF theory had previously been extended for other studies.

Like previous CSF studies, the basis of this study evolved as data was analysed and an increased understanding of the subject was obtained. A conceptual framework was defined after the literature review phase of the study. Subsequently, the framework was refined based on the outcome of the second and third phases of the research methods. This was in-line with the structured-case theory as defined by (Carroll and Swatman, 2000). The structured case approach has been recommended for information systems research as it demonstrates the process of knowledge and theory building by a clear linkage between the data collected and conclusions (Riedl *et al.*, 2007).

The structured-case approach requires the reflection and critical analysis of any interpretations involved and literature-based scrutiny of the findings. The figure below provides an overview of the structured-case process depicting how it was applied to this study.

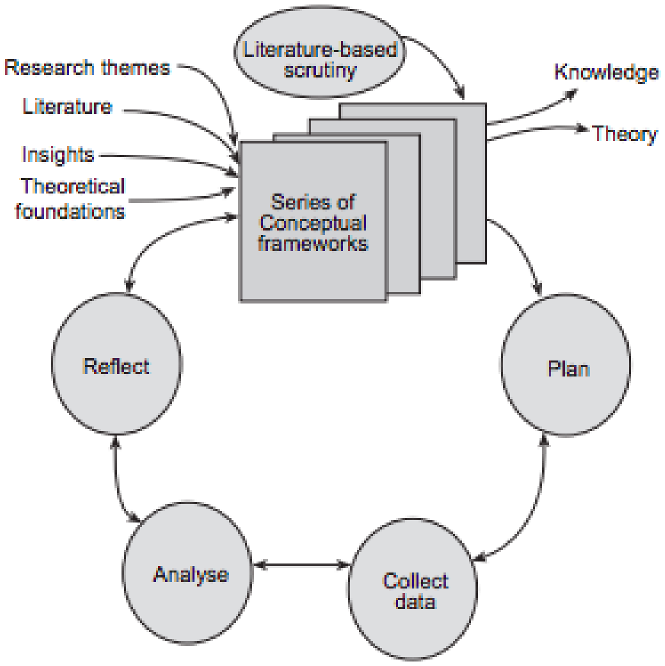


Figure 6.1: Theory Extension Using the Structured-Case Approach (Carroll and Swatman, 2000)

Carroll and Swatman (2000) explains that the interplay between the conceptual framework and research methods provides for building knowledge. From the figure above, 'CF1' depicts the initial conceptual framework based on the researchers understanding. This then formed the preunderstanding for the next research cycle.

Subsequent cycles involved refinement of the framework resulting in a series of conceptual frameworks.

The approach entailed an iterative process which was guided by various input during data collection exercises and further scrutinised by literature. The defined framework formed an extension of the CSF theory which identified the organisational factors that banks should implement to prevent e-banking frauds in Nigeria. Outputs from the theory extension by research phase is summarised by the following diagram.

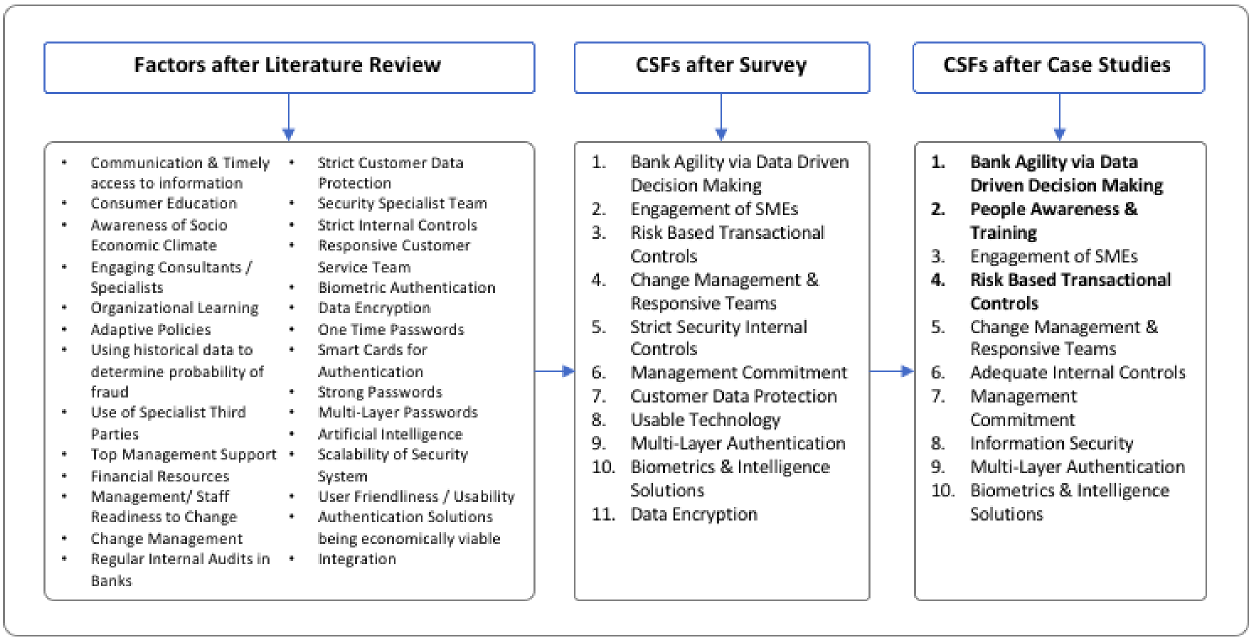

Factors after Literature Review
CSFs after Survey
CSFs after Case Studies
• Communication & Timely access to information
• Consumer Education
• Awareness of Socio Economic Climate
• Engaging Consultants / Specialists
• Organizational Learning
• Adaptive Policies
• Using historical data to determine probability of fraud
• Use of Specialist Third Parties
• Top Management Support
• Financial Resources
• Management/ Staff Readiness to Change
• Change Management
• Regular Internal Audits in Banks
• Strict Customer Data Protection
• Security Specialist Team
• Strict Internal Controls
• Responsive Customer Service Team
• Biometric Authentication
• Data Encryption
• One Time Passwords
• Smart Cards for Authentication
• Strong Passwords
• Multi-Layer Passwords
• Artificial Intelligence
• Scalability of Security System
• User Friendliness / Usability
• Authentication Solutions being economically viable
• Integration
1. Bank Agility via Data Driven Decision Making
2. Engagement of SMEs
3. Risk Based Transactional Controls
4. Change Management & Responsive Teams
5. Strict Security Internal Controls
6. Management Commitment
7. Customer Data Protection
8. Usable Technology
9. Multi-Layer Authentication
10. Biometrics & Intelligence Solutions
11. Data Encryption
1. Bank Agility via Data Driven Decision Making
2. People Awareness & Training
3. Engagement of SMEs
4. Risk Based Transactional Controls
5. Change Management & Responsive Teams
6. Adequate Internal Controls
7. Management Commitment
8. Information Security
9. Multi-Layer Authentication
10. Biometrics & Intelligence Solutions

Figure 6.2: Summary of EBFP CSF after Research Phases

The figure above provides an overview of the research process that was used to extend theory and arrive at the final CSF. The CSF in bold form part of the unique contribution of this study, identified as new CSF for frauds prevention. The next section discusses the findings related to the CSF identified during the course of the study.

6.3 Key Research Findings

This section consolidates and synthesises the findings of the literature review, survey and case study. It highlights the common themes as well as any contrasting themes for the factors. The possible reasons for similarities and differences are discussed and the contribution of the CSF theory in relation to this study is outlined. Generalisations are made specifically in the context of this research which spans retail banks in Nigeria who offer a variety of e-banking services.

6.3.1 E-Banking Fraud Security Challenges

To recap, the initial literature review identified e-banking fraud challenges such as internal fraud, hacking, phishing, card skimming and cloning. It was understood that these activities lead to identity theft and subsequently e-banking frauds. The case study further reiterated these challenges and placed emphasis on customers compromising their information in two forms; knowingly and unknowingly. A tendency for customers to knowingly share their personal details with friends or family was increasing their risk of fraud.

The case studies suggested that the more common compromise are the cases where customers unknowingly compromise their details. Customers visiting sites that are insecure was one of the common challenges explained. This has become a tool in which fraudsters use to retrieve the personal information required to carry out fraudulent transactions. Literature also emphasised this as a challenge explaining that advancements in phishing leads to customers falling victim to websites which are near identical to their financial institution's web site (Singh, 2007). This shows that customers are a primary target, likely due to their higher vulnerability compared to the banks.

On the other hand, people knowingly compromising information also formed a major challenge to preventing e-banking fraud. The study found that this is usually in the form of customers sharing their card details, or bank staff deliberately compromising information or systems. These challenges formed the basis upon which banks have built their fraud prevention measures upon. A summary of the identified CSF is given below.

6.3.2 Accepted EBFP CSF

6.3.2.1 Bank Agility via Data Driven Decision Making

Banks use data and risk management to quickly assess and respond to threats. The table below highlights the sub-factors and activities identified for this CSF.

Table 6.1: CSF 1 - Bank Agility via Data Driven Decision Making

Sub-Factors	Activities
• Organisational learning for fraud prevention	• Root Cause Analysis of Incidents • Leverage local and global experience and expertise
• Adaptive Policies, Procedures and Controls	• Clearly defined roles & responsibilities • A risk-based approach to preventing fraud
• Timely access to information to empower management decision making	• Periodic E-Banking Fraud Reporting • Access to Industry Insights • Fraudulent Events Tracking • Trends analysis and Triggers

Findings from the survey phase revealed that factors relating to this CSF were amongst the highest EBFP criticality ratings for strategic factors. Given the dynamic nature of technology and security, all banks confirmed that it was essential for them to be able to quickly react and be dynamic. This can be in form of being proactive or reactive, learning from past incidents or breaches. A risk management approach to assess risks and prioritise changes have been adopted by banks. Additionally, ensuring that a Root Cause Analysis is carried out when incidents have occurred is deemed essential as the outcome can require changes to bank policies or procedures. Williams (2014) recommends that security policies, plans and procedures are reviewed on a regular basis, indicating the dynamic nature of the field and this aligned closely with the messages given by the banks.

CSB-1 highlighted that risk management was important to the banks agility and explained that regular risk assessments was effective for e-banking fraud prevention. It was emphasised that the risk identification process involved key stakeholders of different departments such audit, IT, risk, security and HR. Literature also suggests that risk management is important for preventing fraud. Mohd-Sanusi *et al.* (2015) had carried out a fraud study in banks and also found that risk management and corporate governance were important for preventing fraud. Monica (2014) recommended that fraud related risk assessments should involve assessing vulnerabilities by assessing culture, attitude and awareness of employees. Therefore, suggesting the need to pay close attention to internal risks to the banks as well as external. Raju and Murthi (2011) recommended an anti-fraud risk process which also proposes a risk driven approach to identify and mitigating fraud risks. Additionally, banks need to have a sense of awareness to the types of cyber security attacks so that they can employ adequate resources to identify and mitigate the risks. Hence reiterating the need for banks to involve the right stakeholders during the risk identification process.

Monitoring industry fraud trends Pandy (2017) has been suggested as a means of preventing fraud. The banks see this as an essential activity to provide them with the opportunity to benchmark themselves across the industry. It helps empower the banks to understand patterns, trends and provides insights on areas that they may need to be strengthened within their environment. Overall the banks review statistics relating to e-banking fraud from daily to monthly depending on the departments, with stakeholders from top management and executive levels reviewing them on a quarterly basis, at minimum. Banks are moving away from only tracking cases of fraud to also tracking suspicious and failed fraud attempts. This is one example of how banks are continuing to collate and use data to be more agile and proactive to threats. Therefore, the banks' ability to learn and adapt is critical to successfully preventing fraud.

6.3.2.2 People Awareness & Training

People have been singled out as a huge risk for banks. Banks identify stakeholders to instil awareness and prevent exposures leading to e-banking frauds. The table below highlights the factors and activities identified for this CSF.

Table 6.2: CSF 2 - People Awareness & Training

Sub-Factors	**Activities**
• Consumer Education	• Sharing Key Messages Continuously • Reaching Customers Through Multiple Channels
• Employee Awareness & Training	• Implement Role Based Training • Develop Awareness on Whistleblowing, Ethics and Consequences of Fraud

The literature review revealed numerous literatures advocating for consumer awareness. Although the factor was rated high in terms of criticality during the survey, several other factors were rated higher by respondents. However, the case study appeared to contradict this as this topic was given high amount of emphasis by the banks. Rather than consumer awareness, the case study findings suggested that the scope of those involved in awareness should include other stakeholders such as bank employees and merchants. Banks undergo consumer, staff and merchant awareness campaigns to keep their risk exposure to a minimum. Awareness campaigns are executed through a combination of mediums to share key messages. Two main types of messages were being communicated by the banks. The first involves making people aware of how to protect information. The second involved making people aware of what to do in the event of a fraudulent incident, immediately they occur, as also recommended by (Javelin, 2017). A summary of the key messages that the banks project to their customers have been covered in the previous chapter, section 5.7.1.4.

For bank staff, periodic awareness trainings and workshops are carried out by the banks, and in some cases the employees are assessed to confirm their understanding. Online training courses and awareness via intranet portals were effective. Tse *et al.* (2013) carried out a study on education in IT security and recommended that bank staff at different levels should be made aware of the importance of corporate security to secure information and assets. Additionally, fraud prevention training has been found to be one of the most effective measures for preventing fraud (Efiong *et al.*, 2016). This is in tandem with the approach that banks are taking.

With regards to awareness and training content, bank staff are being made aware of the implications of not abiding by policies and how it puts customers at greater risk. Additionally, awareness of whistle-blower policies encourages staff to report any suspicious activities and pay attention to disgruntled employees. Okoye (2017) recommends that whistle blowers should be protected against victimisation and defamation so that they can disclose illegality with confidence. Banks have not only adopted this but also reassure their stakeholders of confidentiality and protection.

Another topic covered is that of ethics. Enofe *et al.* (2017) found that compliance with ethics can have significant influence on fraud prevention. Obstfeld and Rogoff (2009) recommends that high ethical standards should be implemented to prevent fraud and therefore should be included within the training. Similarly, Raju and Murthi (2011) had investigated in to fraud cases in India and recommended the need for ethical values to be imparted to internal employees. Monica (2014) also called for organisations to adopt an ethical environment and culture to prevent fraud. Taiwo *et al.* (2016) recommended that banks should continuously train and retrain their staff on issues of morality, trustworthiness and sincerity. Therefore, suggesting that this should be a continuous process for banks.

Furnell and Vasileiou (2017) highlighted that breach after breach, the impact of human factor is being shown and their study found that more needs to be done in security awareness and training.

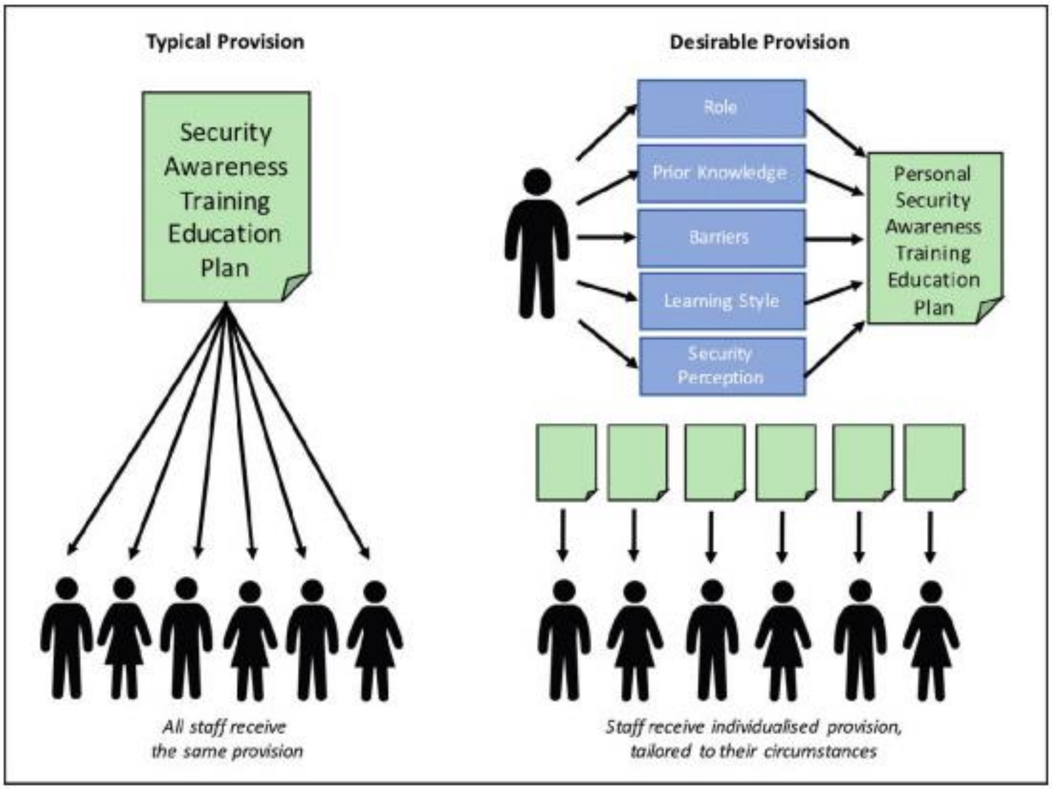

Typical Provision
Desirable Provision
Security Awareness Training Education Plan
Role
Prior Knowledge
Barriers
Learning Style
Security Perception
Personal Security Awareness Training Education Plan
All staff receive the same provision
Staff receive individualised provision, tailored to their circumstances

Figure 6.3: Personalised Approach to Security Awareness (Furnell and Vasileiou, 2017)

Figure 6.3 depicts a personalised approach to security awareness where information such as peoples' roles and prior knowledge are considered. In a similar vein, banks have begun tailoring awareness and trainings to its customers, suppliers and staff to better meet its objectives

6.3.2.3 Engagement of Subject Matter Experts

Securing electronic channels require a broad range of skills and expertise. Banks engage specialists and develop skills to meet up with the high demands and expertise required. The following table highlights the factors and activities identified for this CSF.

Table 6.3: CSF 3 - Engagement of Subject Matter Experts

Sub-Factors	**Activities**
• Engaging Consultants & Specialists	• Adopt strategy to fulfil and maintain security requirements

	• Continuous Skills Development of Staff • Source Specialist Skills
• Awareness of Socio Economic Climate	• Awareness of External Factors • Stakeholder Engagement

The literature review phase found that there a variety of ways which banks can engage experts for EBFP ranging from employing consultants for impartial advice or to implement a system. The case study revealed that all the banks took the need for a security team seriously albeit acknowledging the variety of skills and expertise that is required. The banks differed in terms of how the teams were setup internally to offer security skills, but all had a clear approach as to how they would source security skills to secure their environments. The need for external expertise was common across all banks in addition to continuously developing the skills of their own staff.

Due to the variety of skills required to secure data, the banks all chose to employ the use of consultants. They have particularly been used to enable banks to quickly reach certification of security standards and maintain them. Additionally, consultants provided the banks with independent assessments and specialised areas such as penetration testing. Another area where subject matter experts have been engaged is for site visits, conferences and guidance.

Banks all took collaboration seriously and referred severally to the growing impact of the fraud forum which is bringing together the banks and other key stakeholders in the industry to collectively prevent e-banking fraud. Stakeholder engagement has enabled the banks to also keep abreast of the socio-economic environment. External factors such as this are continuously monitored so that the banks consider them during risk assessments and can adapt accordingly.

6.3.2.4 Risk Based Transactional Controls

Banks are adopting a risk-based approach to secure transactions as a more effective approach than static security criteria. The table below highlights the factors and activities identified for this CSF.

Table 6.4: CSF 4 - Risk Based Transactional Controls

Sub-Factors	Activities
- Using historical data to determine probability of fraud during each transaction	- Implementation of a fraud prevention & monitoring solutions - Introduce additional controls for higher risk transactions
- Use of specialist third parties for online transactions to enhance confidentiality.	- Implementation of additional security measures offered by third parties - Leveraging their expertise for fraud investigations

Fraud prevention solutions have been identified as critical for preventing fraud as banks can now use data to help make more informed decisions, such as predicting whether a transaction is fraudulent, before it occurs. This can be done via behavioural analytics and transaction monitoring. The first part of this is using data to understand patterns of customers and fraudsters to predict fraud. Pandy (2017) suggested that behavioural analytics considers the normal behaviour of the customer, calculates the risk of the activity and introduces intervention measures for the risk before the customer can complete the transaction. The case study did show that the banks had begun implementing such solutions to reduce fraud. The survey analysis found that the 'Using historical data to determine probability of fraud during each transaction' factor obtained the highest criticality rating amongst all 28 factors that were rated, reiterating its perceived significance.

All banks confirmed that they were using third parties and benefiting from some of the investments that the third parties had made in their infrastructure. Some of the organisations mentioned are servicing banks worldwide and therefore can draw from a variety of experiences to help guide their customers or partners. Therefore, banks should leverage such expertise and infrastructure to further enhance security for their transactions.

Pandy (2017) also suggests that data should be used more effectively has to predict fraud. Its suggested that order to achieve this, banks need to go beyond the traditional data which was stored about customers, storing details such as biometrics, geolocations, IP addresses and other details which may be captured during transactions. Due to the sensitivity of this data, it is more imperative that the data being used is stored and transmitted securely, to not pose any unwarranted risk to their customers or even their infrastructure.

Transaction monitoring is the second area which provides insights to feed into the decision-making process of fraud prevention solutions. This also involves analysing transaction data by monitoring information such as unique accounts, cards being used by devices and information such as geolocations and IP addresses. Although, the deployment of such solutions was in its early phases, all research methods consistently found the factor to be critical for EBFP. The banks also expected further reliance of such solutions over time.

6.3.2.5 Change Management & Responsive Teams

Change management is important in a dynamic environment where offerings, technology and threats are ever changing. Banks have responded to this challenge by developing processes and teams that can quickly react. The table below highlights the factors and activities identified for this CSF.

Table 6.5: CSF 5 - Change Management & Responsive Teams

Sub-Factors	**Activities**
• Management & Employee Readiness to Change	• Appoint Primary Drivers for Fraud Prevention • Early Management Involvement
• Change Management	• Lean Change Management Process • Expedite High Priority Changes
• Responsive Customer Service Team	• Providing 24-hour channels for customers to report incidents • Aligning internal processes to urgently address to reported incidents

Early management involvement and identifying key sponsors has helped banks tackle fraud. Two of the banks had appointed members of their top management team playing as key sponsors for fraud prevention, resulting in increased participation and lower lead times for approvals. This approach allows management to be involved, rather than simply being briefed. It also emphasised the importance management are giving to security and fraud prevention. Ramakrishnan (2001) emphasised that the board and senior management should establish effective management control over e-banking risks. The case study banks appeared to agree with this as management have established change management processes that allows changes to be prioritised and implemented with the level of urgency as required.

Although the case study revealed that banks had processes to report and investigate fraud, literature suggests that more can be done to further encourage change. Obstfeld and Rogoff (2009) suggests that staff who are found to be involved in fraud should be prosecuted by their organisations to help act as a deterrent to others. (EY, 2016) also found that 83% of executives believed that prosecuting individuals helps deter fraud. Interestingly, none of the case studies highlighted the importance of prosecuting those involved in fraud. However, literature suggests otherwise emphasising that a culture where those who commit fraud are punished should be enforced to prevent fraud. Its mentioned that a zero-tolerance policy goes a long way in reducing the risks of any illegal activities (Bhasin, 2016).

The case study banks believed that being responsive is vital for preventing fraud in e-banking. They acknowledged that the window to mitigate the risk of fraud after a suspicious activity has taken place can be extremely short. As a result, the banks have all provided a means for customers to contact them 24 hours a day for fraud related matters. The banks introduced notifications informing customers of events leading to transactions. The notifications included guidance on what customers should do is one of the ways the banks achieved this. The banks all established processes to minimise issues and also investigate the root cause to prevent a similar occurrences' in the future. CSB-1 for example reiterated that their capability of cancelling cards immediately after being informed by its customers.

6.3.2.6 Adequate Internal Controls

Internal controls have been continuously strengthened to prevent internal fraud. Furthermore, banks have implemented processes to test compliance and the effectiveness of the controls. The table below highlights the factors and activities identified for this CSF.

Table 6.6: CSF 6 - Adequate Internal Controls

Sub-Factors	**Activities**
• Strict Internal Controls	• Limiting Staff Authority – Segregation of • Role Based Background Checks for Staff • Anonymous Whistleblowing Procedure • Risk Assessing new products • Biometric Verification
• Regular Internal Audits	• Audits that cover full scope of controls • Controls Quality Assessments • Self -Assessments

Banks recognise the importance of internal controls in preventing fraud. This aligns with studies by Okaro *et al.* (2017) and Enofe *et al.* (2017) where it was highlighted that internal controls are a measure that can be effective in preventing fraud. The survey results revealed higher emphasis on strict internal controls compared to the factor suggesting that internal audits should be regular. This suggests that the primary focus should be to ensure the controls are adequately mitigating risks. The case studies revealed that the banks have introduced many common controls to help mitigate the risk of fraud. There are highlighted below.

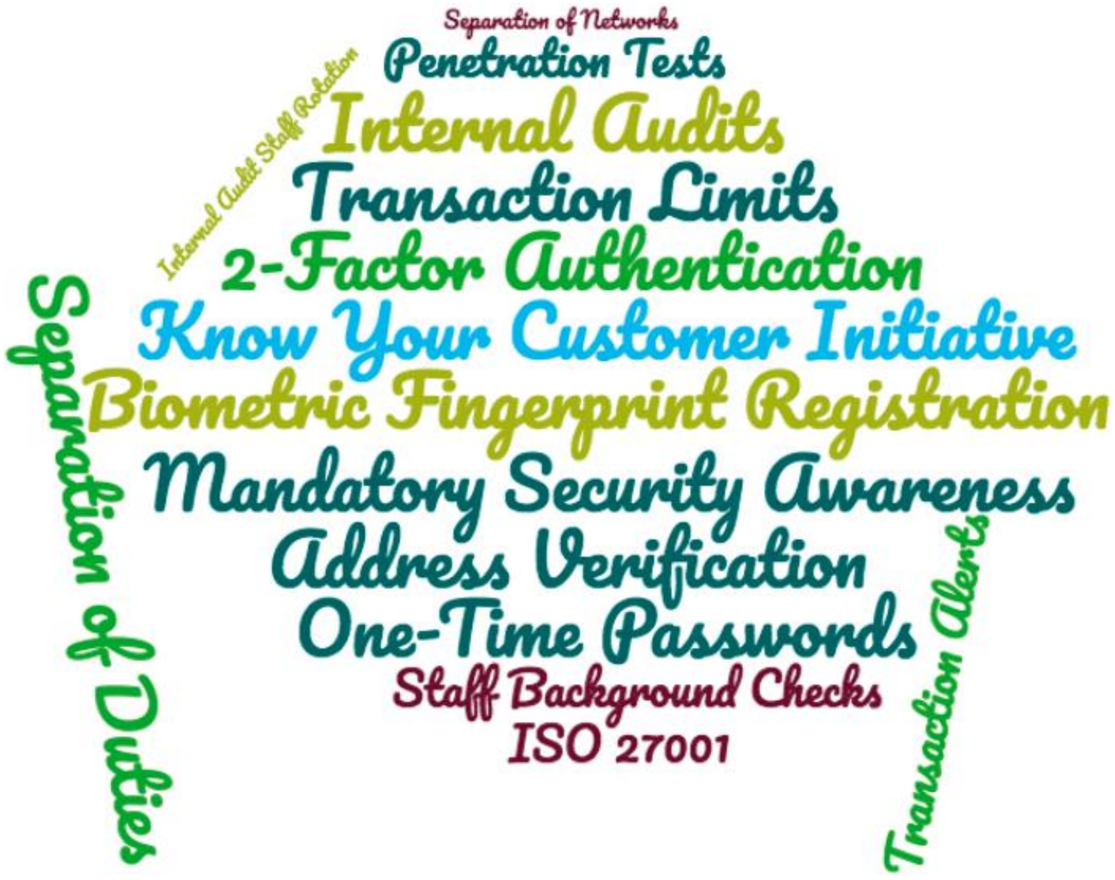


Figure 6.4: Common Bank Internal Controls

Many of these controls relate to banks limiting the authority provided to one member of staff and ensuring that they cannot initiate and complete certain transactions on their own. This aligns with suggestions by Bhasin (2016) who investigated into fraud prevention in banks should implement strict internal controls such as rigorous approval processes and separation of duties.

The whistle blower policy is a control implemented to allow staff or members of the public to report cases for investigation. Akpan (2013) recommended that banks adopt a structure that allows management to be investigated where its deemed necessary, and such a policy should enable this to take place. Verizon Enterprise (2015) highlights whistleblowing as the top method for exposing fraud. In terms of implementing the policy, insights from the case study bank suggest that awareness of the policy, ease of submitting claims and confidentiality were key to its effectiveness.

Although these controls all support with the prevention of e-banking fraud, CSB-3 confirmed that some have not been introduced specifically for e-banking fraud prevention, such as internal audits. However, the scope of the audits has evolved to include e-banking related processes. In contrast, it was highlighted that some controls were specifically for e-banking fraud prevention such as activity notifications & transaction alerts. Okaro *et al.* (2017) supports the structure that the case study banks adopted recommending that audit teams should report directly to management to ensure independence. Additionally, scope, professional competence, examination process and management support were also deemed to be factors for ensuring internal audits are effective.

Separation of duties introduces the concept of requiring more than one person to complete tasks, to prevent fraud. Ramakrishnan (2001) and Yibin (2003) reiterate that segregation of duties is vital for preventing fraud in banks. Banks also confirmed the enforcement of strict access rights to grant staff only to systems, applications and data they need to carry out their responsibilities. Hamidi *et al.* (2013) found that enforcing mandatory access control helps strengthen e-banking security and recommends that banks adopt an architecture to support this whilst also enforcing their IT policies. Additionally, employee access should be revoked immediately they leave (Verizon Enterprise, 2016), leaving no time for misuse. This aligns with one of the practices that CSB-3 implement when staff leave the bank.

After adequate internal controls have been established, there is need for banks to monitor the adherence to these controls by internal audits. The banks explained that regular audits enable a wider scope of controls to be covered. Additionally, self-assessments enable branches and departments to actively appraise themselves and improve even prior to any internal audits that may take place, encouraging continuous improvement in a changing environment.

6.3.2.7 Management Commitment

Top Management Support was deemed critical for preventing e-banking fraud. Banks have adopted ways of including management in the process, rather than simply keeping them informed. The table below highlights the factors and activities identified for this CSF.

Table 6.7: CSF 7 - Management Commitment

Sub-Factors	**Activities**
• Top Management Support	• Obtain initial top management support • Establish regular forums with top management to maintain support
• Financial Resources	• Cost benefit analysis for new investments • Demonstrations & Proof of Concepts

Unanimously, all the bank staff interviewed identified that Top Management Support is a critical factor for preventing fraud for their ability to provide resources, financial or non-financial. Similarly, the two sub-factors related to the CSF were rated highest in criticality for operational factors. Insights obtained from the case study indicated that there were two stages to achieving the desired management support. The first was in respect to obtaining the initial support and then secondly maintaining this support from management. Examples of scenarios of how top management support was achieved were provided in chapter 5. Essentially, management must understand the importance of preventing fraud and understand that it is a continuous process. A recurring theme was that banks had established a regular forum with members of the top management team so that fraud issues and mitigations could be discussed.

One of the most common references made whilst providing examples of management support, was in the form of financial resources. The banks rely on management to provide approvals and budget allocations to improve their controls. CSB-2 highlighted proactivity at times required large investments to be made without management necessarily understanding the threat being experienced, hence making it difficult to justify. In an attempt to overcome this, banks have adopted similar strategies; Firstly, cost benefit analysis are carried out to help the management understand the costs involved and compare them against the expected benefits. Secondly, the banks involve management in demonstrations, site visits and proof of concepts as a means of evidencing the expected value for the investment being proposed.

For this CSF, the researcher believed that the term management "commitment" was more suited to the findings of the study. This is because top management are engaged in governing the risks associated with fraud prevention requiring their commitment in the form of time and finances.

6.3.2.8 Information Security

Several controls identified by the study relate to securing information. Banks are adopting a combination of standards to secure their channels as they transact with customer data. The table below highlights the factors and activities identified for this CSF.

Table 6.8: CSF 8 - Information Security

Sub-Factors	**Activities**
• Strict Data Protection	• Implement an Information Security Management System • Secure Channels for Card Present & Card Not Present Transactions • Data Encryption
• Adoption of International Security Standards	• Adopt Chip & PIN platform such as EMV • Adopt standard such as PCI DSS and PCA DSS for protecting Card Data • Adopt an Information Security Management System such as ISO 27001

The open-ended questions section of the survey questionnaire led to the identification of factors relating to information security. Factors such as EMV and PCI DSS were introduced at this phase by multiple respondents. Subsequently, the case study further revealed additional activities which banks have been undertaking to achieve information security and prevent fraud. Information security can be described as the technical methods and managerial processes covering hardware, software and data to protect organisational assets and personal privacy (Hong *et al.*, 2003). Banks placed emphasis on activities or initiatives to secure customer data. There was not one standard or solution to fit all security requirements but rather a combination of measures being used.

Data breaches have resulted in added emphasis and recommendations on the importance of data being encrypted (Crosman, 2017). Data encryption was emphasised as measures taken by all banks and also forms a requirement for many of the security standards the banks adopted. Customer data protection is also a priority for the banks, but other data types are also considered and protected. CSB-2 had explained that a compromise in non-customer data and systems may subsequently lead to customers data being compromised. Therefore, all data types are considered and secured using an information security management system.

The Payment Card Industry Data Security Standard (PCI DSS) is a set of requirements designed to ensure companies that are involved in processing, storing or transmitting credit/debit card information, maintain a secure environment to guarantee the protection of cardholder data throughout the whole transaction process. The standard also facilitates the broad adoption of consistent data security measures globally and the certification is renewable annually as required by the Payment Card Industry Council. CSB-1 confirmed that the PCI DSS standards are not only followed but recertified when due. This shows the bank’s commitment to ensuring that sensitive data is secured. According to the CSB-1, “the Bank will strive to continually maintain leading best practice and secure customers’ information despite the challenges posed by rapid changes in technology and the operating environment” - Press Dossier. This shows that their top management understands the dynamic environment and their commitment to maintain security.

Migration to a chip and pin environment was another measure that the banks implemented to strengthen the security of card transactions. Ultimately, the drivers to migrate to EMV do fall back to either fraud or marketing-related drivers (Povey, 2008). The primary issue reported was that cards were being cloned and exploited. All the case study banks confirmed that magnetic strip cards were prone to cloning and had experienced incidents of fraud. This was a common issue with the magnetic strip cards as fraudsters had started creating counter magnetic stripes using information from discarded sales slips as far back as 1993 (Arend, 1993).

Ever since the introduction of EMV, all banks reported reduced e-banking fraud rates, particularly at ATM machines. This is in-line with global chip and pin migrations such as countries like France and Malaysia (Povey, 2008). Initially, the bank had left the fall-back option for the EMV cards to magnetic active, however due to frauds that occurred internationally the policy was changed. The fall-back option was then only made available on request, customers had to apply officially as the banks shift liability to them. This challenge was not unique to Nigeria. In the UK even after the migration to Chip and Pin, the technology was subject to criticism due to the remaining magnetic strip cards and devices that were still in use, but not actually due to the chip & pin technology (Card Technology Today, 2006). Although EMV has been deemed successful in reducing card cloning, it has led to fraudsters focussing their attention to card not present transactions (Javelin, 2017).

6.3.2.9 Multi-Layer Authentication

Multiple layers of passwords strengthened banks authentication processes, particularly for card not present transactions. Banks tended to implement a combination of traditional passwords and OTPs. The table below highlights the factors and activities identified for this CSF.

Table 6.9: CSF 9 - Multi-Layer Authentication

Sub-Factors	**Activities**
• Multi-Layer Passwords	• Implement a minimum of 2-Factor Authentication (One pre-set and one from an OTP) • Password policies should be enforced
• One Time Passwords	• Adopt OTPs for customers and staff • OTPs generated by the bank systems should be sent to pre-registered devices

Strong authentication systems have been highlighted severally as important measures to prevent fraud. A combination of knowledge based, One-time passwords and passive authentication methods such as geolocation and biometrics help strengthen the authentication process. All the case study banks had implemented a minimum of 2 factor authentications combining passwords with one-time passwords which were either generated by the user or sent to them via SMS to a pre-registered phone number or email. The majority of the case study banks used one-time passwords to also authenticate their staff.

6.3.2.10 Biometrics & Intelligence Solutions

Biometrics and fraud prevention solutions were highlighted as important technologies for preventing e-banking fraud. Although the case study revealed signs of early adoption, benefits of such technologies have already been experienced. The table below highlights the factors and activities identified for the final CSF.

Table 6.10: CSF 10 - Biometrics & Intelligence Solutions

Sub-Factors	**Activities**
• Biometrics to strengthen authentication system	• Biometric database • Biometric authentication via mobile
• Artificial Intelligence to predict, alert and prevent fraud	• Transaction alerts • Leverage transactional and geological data to determine fraud probability

All banks were going through a fingerprint biometric registration exercise as mandated by the Central Bank of Nigeria. Although this was a mandatory requirement by the regular, the banks did feel it was an important step towards utilising fingerprint biometrics for customer authentication. Two of the banks confirmed that they had already been considering biometric authentication, although cost appeared to be one of the major hindrances. During the case studies, all reference to biometrics were in the form of fingerprint technology. However, literature suggests that behavioural biometrics such as keystroke dynamics may also have a role to play in preventing fraud. In addition, technology companies such as IBM have begun incorporated behavioural biometric capabilities to prevent fraud by understanding how user interact with banking websites (Biometric Technology Today, 2016).

Although biometric technology does provide an opportunity to strengthen authentication, it too has its challenges. For example, Jain *et al.* (2006) gave an example that a super user may modify parameters of the system to permit intrusions and gave circumvention and coercion as other examples. However, the research concluded that it has potential to have a profound influence on the way we conduct our business by ensuring information security. It has also been recommended that biometric technology is used in conjunction with other authentication measures. Onyesolu and Okpala (2017) recommends a three-tier approach to authentication at ATMs using biometrics and passwords. Similarly, Omogbhemhe and Bayo (2017) recommended that fingerprint biometrics should be combined with another layer of security to address the risks of using biometrics alone for authentication. In contrast, it has also been proposed that the introduction of biometrics alone at ATMs would further strengthen authentication and prevent fraud (Oye, 2018). Although there doesn’t appear to be a consensus on whether biometrics should be coupled with additional tiers of authentication checks, all studies agree that it does strengthen the authentication process.

An important activity that all the banks referenced were notifications to their customers. These inform the customer when they have logged into their online banking and when a transaction is initiated. This provides the customers with a window to react if the action had not been carried out by themselves prior to a financial transaction taking place. Although it is not used as part of the steps to authenticate the customer, the banks believed that it was a measure that helps strengthen the authentication process to prevent fraud. The only exemption to this was when customers were using their cards at ATMs or POS devices to make payments. In such scenarios the notifications were being sent after the transactions had taken place.

Fraud prevention software was an area where the banks felt had begun to play a key role in preventing fraud. Literature suggests that software using artificial intelligence should be used to help prevent fraud. Holzenthal (2017), reiterated that banks should seek help from artificial intelligence and advanced analytics to prevent fraud. Additionally, this factor was one of the highest rated technological factors from the survey questionnaire. The case studies revealed that all the banks had begun utilising fraud prevention software. CSB-3 implemented a database monitoring solution for real time threat detection whilst CSB-2 confirmed that additional controls were being introduced for high risk transactions before they could be completed. Although early in its adoption, the banks all believed in the criticality of such solutions and is a key part of their strategy going forward.

Finally, the cost of systems does play a pivotal role on whether advancing systems are deployed. CSB-1 confirmed that the financial cost of fingerprint biometrics was one of the hindrances to adopting the technology. The banks explained that before investments could be made in authentication systems, or even any technological acquisition, a cost benefit analysis is carried out to aid the decision-making process.

6.4 Rejected EBFP CSF

All factors discussed in the previous section were identified and validated in accordance with the research methods adopted for this study. This supports suggestions from CSF theory, whereby factors were validated by multiple sources before being confirmed. However, during the research process, the following factors did not receive enough supporting evidence to be confirmed by this study. This is discussed below:

- Usable Technology – Findings from both the survey results and interviews suggested that although the factor was considered for deploying solutions, it was not deemed critical for preventing e-banking frauds. In addition, it was revealed that this is a factor considered by the banks when adopting solutions to offer services to customers that are easy to use. However, there was no evidence to suggest its significance for preventing e-banking frauds across multiple phases of the research.

6.5 CSF-Based EBFP Framework (final)

This section outlines the revised CSF-Based E-banking Frauds Prevention framework after the final phase of the research methodology. The refined CSF and sub-factors are depicted in figure 6.5 below:

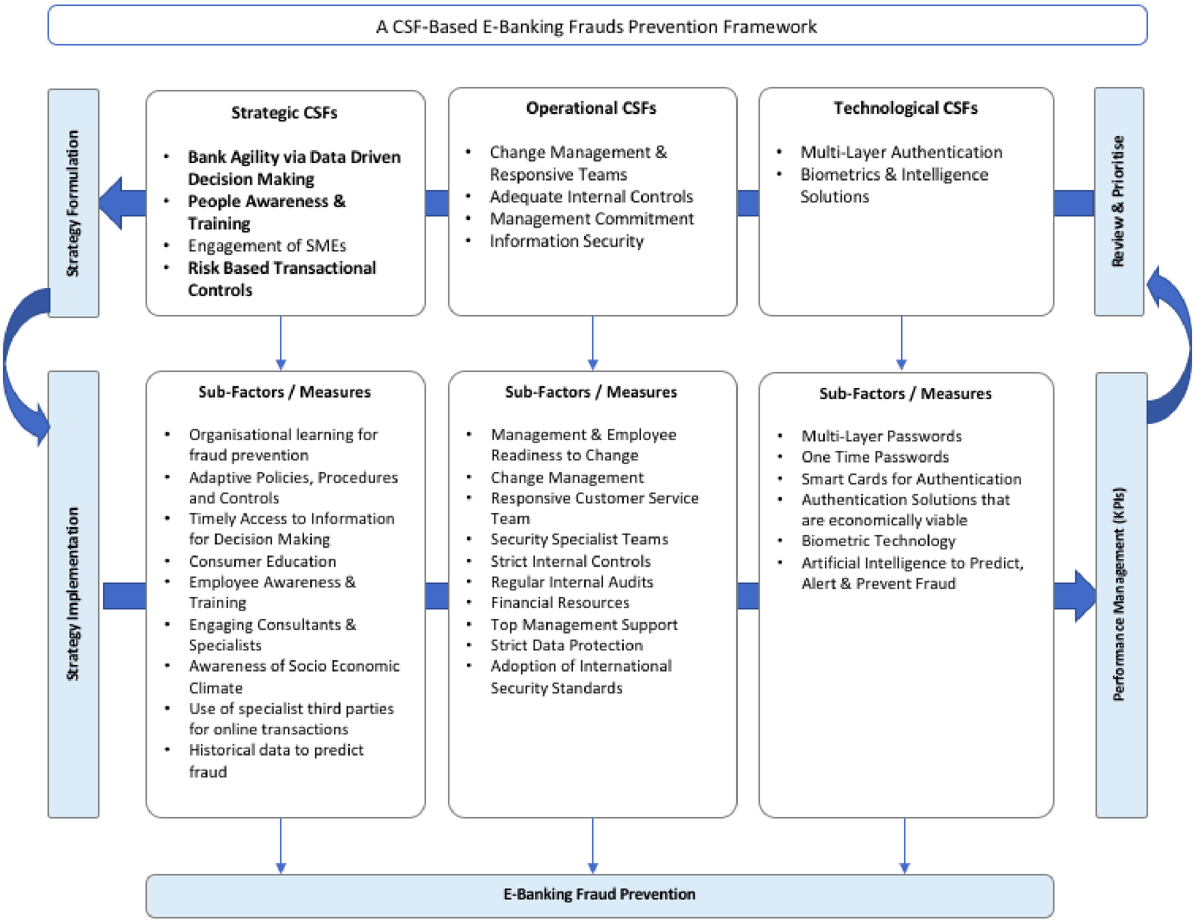

A CSF-Based E-Banking Frauds Prevention Framework
Strategy Formulation
Strategic CSFs
Bank Agility via Data Driven Decision Making
People Awareness & Training
Engagement of SMEs
Risk Based Transactional Controls
Operational CSFs
Change Management & Responsive Teams
Adequate Internal Controls
Management Commitment
Information Security
Technological CSFs
Multi-Layer Authentication
Biometrics & Intelligence Solutions
Review & Prioritise
Strategy Implementation
Sub-Factors / Measures
Organisational learning for fraud prevention
Adaptive Policies, Procedures and Controls
Timely Access to Information for Decision Making
Consumer Education
Employee Awareness & Training
Engaging Consultants & Specialists
Awareness of Socio Economic Climate
Use of specialist third parties for online transactions
Historical data to predict fraud
Sub-Factors / Measures
Management & Employee Readiness to Change
Change Management
Responsive Customer Service Team
Security Specialist Teams
Strict Internal Controls
Regular Internal Audits
Financial Resources
Top Management Support
Strict Data Protection
Adoption of International Security Standards
Sub-Factors / Measures
Multi-Layer Passwords
One Time Passwords
Smart Cards for Authentication
Authentication Solutions that are economically viable
Biometric Technology
Artificial Intelligence to Predict, Alert & Prevent Fraud
Performance Management (KPIs)
E-Banking Fraud Prevention

Figure 6.5: CSF-Based E-Banking Fraud Prevention Framework (final)

The framework outlines that a total of 10 CSF for E-Banking Frauds Prevention in Nigeria was confirmed. The framework also includes the interrelated sub-factors which were identified and validated over the studies research methods. These have been discussed within the previous sections of this chapter. In terms of CSF application, the framework highlights that the implementation of CSF is a continuous process. CSF should be reviewed and prioritised based on each organisation and their current level of implementation. During the strategy formulation process, organisations should agree on specific measures which will be implemented to achieve the CSF. Importantly, theory suggests that the performance of implemented CSF should be monitored.

6.6 Chapter Summary

This chapter has discussed the findings from the previous phases of the research. It also explained how the structured-case approach was used to extend theory. This helped bring together findings from the different research phases and critique the findings with literature. The triangulated research process resulted in refinements to the CSF after each research phase. CSF were identified and discussed along with their related sub-factors and activities. The case studies helped obtain a deepening understanding of the CSF and obtain additional insights from bank personnel. The factors which were not commonly believed to be critical were also discussed. This chapter helped address the following research question:

Research Question 5: How do organisations achieve the identified critical success factors to prevent e-banking frauds?

A total of 10 CSF was identified, although these were strictly reflective of the findings of this study and its limitations. It also formed the basis for the development and refinement of the conceptual CSF-Based EBFP Framework before arriving at the final iteration for this research. The fact that these factors had been reviewed and validated by industry professionals of whom had first hand experiences in preventing e-banking fraud, provided further credibility to the results.

Strategic factors disclosed that banks are using data to be more agile and make smarter decisions based on risk. It suggests that banks should have timely access to information to help make those decisions, but also setup organisationally to be able to implement adaptive policies and procedures. Similarly, it was found that banks should introduce controls based on risks of transactions. There was an emphasis on the threat of people which requires continuous awareness relating to activities they should and shouldn’t do. On the contrary, people have also been identified as pivotal in preventing fraud and banks should source specialist skills to enable them to do so.

Operational factors revealed an emphasis on management commitment and adequate controls. A recurring theme was the need for banks to continuously assess and strengthen their controls to keep up with changing risks. In order to achieve this, management commitment is deemed critical. Top management should be involved and not only informed. There is a requirement for continuous top management engagement for responsiveness and prioritisation of resources as necessary. The study found that information security plays an important role as the banks focus on adopting international security standards to secure their transactions and infrastructure.

It has been mentioned that technology can play a major role in preventing fraud (Bhasin, 2015). As anticipated, technological factors were also highlighted as critical for preventing e-banking fraud. The study found that technology is heavily adopted as an enabler for banks to achieve their fraud prevention strategy. Multi-layer authentication was found critical to preventing fraud by strengthening the user authentication process. OTPs and biometric technology were highlighted as measures that help strengthen authentication. Fraud monitoring and prevention solutions are enabling banks to use technology to put higher risk transactions through more stringent controls.

As this study is the first study for CSF for EBFP, it can be argued that all factors are new factors in its context. However, some of the factors have been identified as critical in previous security related research. When compared to these studies, there are 3 new CSF that had not been previously identified. These are Bank Agility via Data Driven Decision Making, People Awareness & Training and Risk Based Transactional Controls which have all been elaborated on earlier within this chapter.

The CSF-Based Framework synthesised the CSF and sub-factors to propose a foundational set of factors that banks should implement to help prevent e-banking fraud. Uniquely, the framework also incorporates guidelines for the application of the CSF in organisations based on existing theory. Therefore, beyond the identification of CSF, the framework also mentions how they should be applied. This study can be used as a platform for future studies to further cement the findings or apply in a different context.

CHAPTER 7: CONCLUSION

7.1 Introduction

Despite several previously developed security frameworks and technologies to prevent fraud, they do not provide the appropriate security required to prevent fraud, especially over e-banking mediums as it remains an issue today. Additionally, a comprehensive frauds prevention framework focussing on e-banking does not exist. Thus, this research set out to address the gap identified by defining an e-banking frauds prevention framework by extending CSF theory.

The research has been able to achieve its aims as defined in Chapter 1, the introductory chapter of this thesis. Firstly, it has identified a set of CSF for preventing e-banking frauds in Nigeria. The identification process involved a phased approach over a series of research methods and data sources. Factors were identified after a comprehensive review of literature and validation by selected bank staff. Secondly, the CSF were used to propose a framework for preventing e-banking frauds. This extended CSF theory and included how the factors should be applied within organisations.

This is the concluding chapter of the research and provides an overall summary of the research whilst reverting to the initial research problem, objectives and research questions. It discusses the research conclusions, limitations and contribution to new knowledge. The chapter provides a reflection on the research process and elaborates on the scope for further research.

7.2 Summary of Research

Banking institutions have embraced e-banking solutions to improve customer service and increase their reach to the customers, but incidents of frauds continue to be an issue resulting in losses to banks and customers. Previous frameworks to prevent fraud have not been able to address the issue leaving the need for additional research. In addition, previous studies revealed that fraud prevention frameworks and measures had been proposed in broad contexts and not specifically for e-banking mediums, identifying a gap in research. Additionally, empirical research on this topic and in the context of Nigeria did not exist.

The research aimed to identify factors critical for successfully preventing e-banking frauds and propose a framework for Nigerian banks. A series of research questions were formed to help achieve the research objectives. Logically, the researcher started by ascertaining a detailed understanding of the challenges experienced in preventing frauds and then an understanding of the measures that have been effective in the prevention of frauds, and how they had been achieved. In summary a total of 5 research questions were defined.

A variety of theories such as Cost Benefit Analysis, CSF, SWOT, KPIs amongst others were considered. The CSF theory, a theory adopted severally for previous information systems research to meet similar objectives was adopted by the researcher. This provided the opportunity to address the identified gap and help banks with findings to support their strategic planning process. The philosophical beliefs of the researcher led to a mixed methods approach to the study.

A systematic literature review identified related literature and they were examined to extract common themes in relation to factors that have been effective in preventing frauds. A conceptual framework was proposed which depicted the initial findings categorised into strategic, operational and technological factors as suggested by previous CSF studies. A total of 28 factors were identified from the literature review with coverage of technological and non-technological factors. ‘Consumer Education’, ‘Top Management Support’ and ‘One Time Passwords’ were some of the factors that were identified amongst others. The findings also formed the basis upon which empirical research was built upon for subsequent research methods.

A survey by questionnaire was the quantitative research method adopted that aligned to the positivism stance of the research phase. The questionnaire was completed by professionals working in banks to rate the criticality of fraud prevention factors identified from the literature review, in the context of e-banking in Nigeria. The survey was administered using an online tool due to the its ability to quickly reach a variety of targeted respondents at their convenience. A total of 110 usable responses was obtained after the survey was administered for a period of 3 months.

Analysis of the data revealed that the highest rated factors were ‘Using historical data to determine probability of fraud during each transaction’, ‘Financial Resources’ and ‘Authentication solutions being economically viable’. The findings from the survey also supported the factors identified from the literature review as all but one of the factors were rated at the higher ends of the scales on average. Inferential analysis using Mann-Whitney and Kruskal-Wallis tests were conducted which resulted in some significant variances between the groups of experience that the respondents had in e-banking security. Although this was only evident for a few factors, it further emphasised the need for engaging stakeholders with varying levels of experience in subsequent research phases. A Principal Component Analysis was used to group similar interrelated factors. The output of this produced a total of 11 CSF and the conceptual framework was refined in accordance with the findings.

The final research method involved a case study of 4 banks in Nigeria. The objective of this phase was to validate the findings from the previous phases of the research and solicit a deepened understanding of the factors. This was achieved via a total of 29 semi-structured interviews and analysis of several secondary data sources to understand how the CSF for e-banking fraud prevention could be achieved. A reflective view on the case study process was provided by the researcher.

Common and contrasting themes from the case study were analysed, evaluated against findings from the previous phases of the research to aid the extension of theory. The output involved the introduction of two new factors and the rejection of another factor. Information security was one of the new factors to be introduced. Activities relating to this factor was introduced during the survey and the case study subsequently revealed that it formed a key role in banks being able to successfully prevent fraud. It was found that the banks had not only adopted information security management systems to effectively manage security risks, they also complemented this with implementations of a series of international standards to secure specific data or transaction types. The second new factor identified was People Awareness & Training. The previous phases of the study had identified consumer awareness as a factor for EBFP. However, findings from the case studies revealed that there was a real emphasis on awareness and training of people. This broadened the scope of this factor necessitating the need for all people that banks engage with to undergo a form of awareness or training.

The study concludes that there is a total of 10 CSF for EBFP in Nigeria. Each of the confirmed CSF were outlined with their sub-factors and activities on how to achieve the CSF based on the findings of the research. The CSF-Based framework was further refined in accordance with the overall research findings. From the factors identified, three of the factors were new CSF that had not been reported in e- frauds prevention related studies. These are ‘Risk-Based Transactional Controls’, ‘People Awareness & Training’ and ‘Bank Agility via Data Driven Decision Making’. A summary on each of the 10 factors, their interrelated sub-factors and activities were discussed in chapter 6 of this thesis.

The next section provides further details on the contribution to knowledge that this study has provided.

7.3 Research Originality & Contribution

The primary contribution of this study is that it has extended the application of the CSF theory to the topic of e-banking fraud prevention in Nigeria. The findings help provide focus on the organisational factors identified as critical to preventing e-banking frauds that banks should consider during their strategic planning processes.

Since banks all have the responsibility of protecting their e-banking channels, there is an incentive to identify the key areas and prioritise their resources to minimise the risks involved in rendering electronic banking services. In order to achieve this, previous literature and experience from banks were synthesised to understand factors that have been most effective. The research objective was achieved by adopting a positivism and interpretivist philosophy applying research methods that aligned with both philosophies.

The originality and contribution of the research can be summarised as follows:

1. The first contribution of this thesis is that it identified a set of CSF for E-Banking Frauds Prevention, the first of its kind. Although previous studies have shown that the CSF theory has been extended in a variety of contexts (Caralli *et al.,* 2004; Torres et al., 2006; Foster *et al.,* 2007; Zafar *et al.,* 2011; Tu and Yuan, 2014; Bobbert and Mulder, 2015), none are in the context of this study, which provides a comprehensive set of factors for banks to successfully prevent e-banking frauds. Furthermore, the study provides detailed empirical accounts of strategic, operational and technological factors that banks should implement.
2. The study synthesised preventative organisational factors and proposed a conceptual framework by combining CSF theory and e-banking fraud prevention factors. The framework provides practical concepts and activities for organisations to achieve the factors. Thereby addressing some of the limitations of CSF theory, extending beyond the identification of a list, which is of limited value. Each of the factors are presented with descriptions and activities for deepening understanding, offering insights on how they can be achieved.
3. The identified CSF offer new concepts based on empirical accounts which have been proposed for preventing e-banking frauds. Amongst these are ‘Risk-Based Transactional Controls’, ‘People Awareness & Training’, and ‘Bank Agility via Data Driven Decision Making’ were identified as new EBFP CSF.
4. The study introduces the issue of variations within criticality perceptions between stakeholders. 7% of the factors rated is the survey revealed statically significant differences by respondents of different experience categories, leaving need for further investigation and consideration for future research

5. The final contribution of this study is that it provides detailed empirical accounts of challenges and successes of e-banking fraud prevention in the context of the Nigerian banking industry, where research in this topic is extremely limited.

Overall, this thesis acts as a useful reference for organisations helping to provide adequate consideration to frauds prevention during their strategic planning. Although the data collection took place in Nigeria, the factors may be relevant in a broader range of contexts providing a basis for further research. Additionally, it may serve as evidentiary data for comparative analysis in environments with social, economic and cultural differences.

The study also offers additional benefits to both researchers and stakeholders working in banks as mentioned in the table below.

Table 7.1: Benefits of this Research

Researchers	**E-Business, IT Security Managers & Executives**
• Identifies an appropriate reference theory for the prevention of E-Banking Fraud Prevention which can that can be applied to other security perspectives such as detection & investigations. • Provides insights into the impact e-banking security working experience has on rating the criticality of CSF	• A common understanding of the challenges associated with E-Banking Frauds Prevention • Organisational CSF for E-Banking Fraud Prevention, categorized into three perspectives: strategic, operational and technological. • A comprehensive framework which provides insights on the EBFP CSF defining how they should be applied, and the key activities involved to achieve them

Overall, the findings will be valuable to people working in e-banking security related occupations in banks or anyone who is involved with addressing the challenge of preventing frauds over e-banking mediums.

Having summarised the contributions of the research, the following table summarises how the objectives of the research have been met whilst referencing the respective chapters where further details on the outcome can be sought.

Table 7.2: Research Objectives & Chapters They Were Addressed

Research Objectives	Chapter Addressed
1. To investigate into the CSF of e-Banking frauds prevention in similar contexts using a literature review	• Chapter 2: Identified factors that may be critical for preventing e-banking frauds via a literature review
2. To identify and validate the CSF for EBFP in Nigeria	• Chapter 4: Rated the factors criticality via a survey of bank staff in Nigeria. • Chapter 5: Validated factors, obtained a deepening understanding from banks and a few additional factors were introduced • Chapter 6: Discussed all findings from research phases and final list of CSF were presented
3. To propose a CSF based framework for preventing e-banking frauds	• Chapter 2: Developed the Conceptual Framework based on the CSF theory and introduced the Structured-Case Approach for Theory Extension • Chapter 4 & 6: The conceptual framework was refined after the survey analysis and case study. Discussion of findings and final framework was presented.

Torres *et al.* (2006) highlighted that technology alone cannot solve security problems but rather an interface between technology, policies, procedures and users. This study has taken cognisance of this and proposed a CSF-Based EBFP framework taking those areas into account. CSF have been used in a variety of fields to help establish areas of priorities for meeting objectives. Examples of these were provided during the literature review phase which spanned from e-banking adoption to security culture and policies. Therefore, emphasising the potential role that CSF can play. The CSF identified in this study provide organisations with issues for careful consideration during the strategic planning process to help reap the desired benefits of an increasingly important challenge, preventing e-banking fraud.

7.4 Limitations and Future Research

This section highlights the limitations of the study as identified by the researcher and proposes areas for future research.

The empirical research was based on data from Nigerian banking industry. Therefore, restricting the generalisability of the findings to Nigerian banks at most. However, the research did find that most the challenges experienced by Nigerian banks were similar to those experienced in various countries worldwide. This may suggest that the factors employed which have been critical may also be critical for other countries also. However, future research should be carried out to confirm this. The methodology adopted in this research should be used to analyse and understand perspectives of stakeholders from other geographies.

Nigeria has a general lack of empirical research in the topic of e-banking fraud prevention. Therefore, there was limited literature available for review and reference during the research process. In addition to the limitations of literature, the empirical research was subject to the following limitations:

- The largest population of respondents from the survey had less than 5 years' experience. Therefore, the results may be biased towards the lesser experienced category of bank personnel.
- A low number of usable responses from the survey was obtained. Additionally, the researcher has access to a limited number of interviewees and secondary data during the case studies.
- The case studies had representation from slightly over 10% of the banks. Therefore, it can be argued that further research is required to determine the general applicability of the CSF to the industry.

It has previously been highlighted that CSF may evolve over time due to changes to environments and therefore they should be periodically re-evaluated (Henderson et al., 1984). This suggests that the relevance and or weighting of criticality may change. These CSF were identified based on the available literature and experiences of bank personnel at the time of the study. There is a need to periodically reassess the CSF and it is anticipated that this study can be used as the foundation upon which further studies can be built upon.

Finally, the CSF covered were primarily internal organisational factors. As the theory suggests, there are additional types of CSF which were not within the scope of this study such as external, industry and socio-economic. Therefore, there is an opportunity to replicate this study to identify other CSF types.

REFERENCES

Abdi, H. and Williams, L.J. (2010). ‘Principal Component Analysis’, *Wiley Interdisciplinary Reviews: Computational Statistics,* **2**(4), pp. 433-459.

Abdou, H., English, J. and Adewunmi, P. (2014). ‘An Investigation of Risk Management Practices in Electronic Banking: The Case of the UK Banks’, *Banks and Bank Systems,* **9**(3).

Abercrombie, R. K., Sheldon, F. T. and Mili, A. (2009). ‘Synopsis of Evaluating Security Controls Based on Key Performance Indicators and Stakeholder Mission Value’. 42nd Hawaii International Conference on Systems Science (HICSS-42 2009), Waikoloa, Big Island, HI, USA.

AbuAli, A. N. and Abu-Addose, H. Y. (2010). ‘Data Warehouse Critical Success Factors’, *European Journal of Scientific Research,* **42**(2), pp. 326-335.

Abubakre, M., Coombs, C. Jayawardhena, C. and Hunt, A. (2010). ‘Learning the Lessons from the Developed World: E-banking Security in Nigeria’, UK Academy for Information Systems, UK.

Abu-Shanab, E. and Matalqa, S. (2015). ‘Security and Fraud Issues of E-banking’, *International Journal of Computer Networks and Applications,* **2**(4), pp. 179-188.

AbuZineh, S. (2006). ‘Success Factors of Information Security Management: A Comparative Analysis between Jordanian and Finnish Companies’, unpublished MSc thesis, The Swedish School of Economics and Business.

Adams, R. (2010). ‘Prevent, Protect, Pursue–a Paradigm for Preventing Fraud’, *Computer Fraud & Security,* **2010**(7), pp. 5-11.

Adeniyi, A. (2016). ‘Analysis of Fraud in Banks: Evidence from Nigeria’, *International Journal of Innovative Finance and Economics Research,* **4**(2), pp.16-25.

Adepoju, A. S. and Alhassan, M. E. (2010). ‘Challenges of Automated Teller Machine (ATM) Usage and Fraud Occurrences in Nigeria–a Case Study of Selected Banks in Minna Metropolis’, *Journal of Internet Banking and Commerce,* **15**(2), pp. 1-10.

Adetiloye, K. A., Olokoyo, F. O. and Taiwo, J. N. (2016). 'Fraud Prevention and Internal Control in the Nigerian Banking System', *International Journal of Economics and Financial Issues,* **6**(3).

Adewale, A., Ibidunni, A. S. Badejo, J. Odu, T. and Adoghe, A. (2014). 'Biometric Enabled E-banking in Nigeria: Management and Customers' Perspectives', *Information and Knowledge Management,* **4**(11), pp. 23-28.

Adewoye, J. O. and Ayo, C. K. (2010). 'The State of E-banking Implementation in Nigeria: A Post-Consolidation Review', *Journal of Emerging Trends in Economics and Management Sciences,* **1**(1), pp. 37-45.

Ackroyd, S. and Fleetwood, S. (eds) (2005). 'Methodology for Management and Organisation Studies: Some Implications of Critical Realism', *In Critical Realist Applications in Organisation and Management Studies,* pp. 142-165. Routledge.

Aggelis, V. (2006). 'Offline Internet Banking Fraud Detection. Availability, Reliability and Security, 2006. ARES 2006'. The First International Conference on Availability, Reliability & Security, Vienna, April.

Agwu, E. (2018). 'The Role of E-Banking on Operational Efficiency of Banks in Nigeria', Available at: https://ssrn.com/abstract=3122498.

Agwu, E. and Carter, A.L. (2018). 'Mobile Phone Banking in Nigeria: Benefits, Problems and Prospects', *International Journal of Business and Commerce,* **3**(6).

Ajayi, I. E. and Enitilo, O. (2016). 'Impact of Electronic Banking on Bank Performance in Ekiti State, Nigeria', *International Journal of Multidisciplinary and Current Research,* **4**.

Akbari, P. (2013). 'A Study on Factors Affecting Operational Electronic Banking Risks in Iran Banking Industry (case study: Kermanshah melli bank)', *International Journal of Management and Business Research,* **2**(2), pp. 123-135.

Akinyemi, O., Omogbadegun, Z. O. and Oyelami, O. M. (2011). 'Towards Designing a Biometric Measure for Enhancing ATM Security in Nigeria E-banking System', *International Journal of Electrical & Computer Sciences,* **10**(6).

Akpan, M. D. (2013). 'The Role of Management in Preventing Banking Fraud in Nigeria', unpublished PhD thesis, Walden University.

Al-Araki, M. (2013). 'SWOT Analysis Revisited Through PEAK-Framework', *Journal of Intelligent & Fuzzy Systems,* **25**(3), pp. 615-625.

Alavi, M. and Carlson, P. (1992). 'A review of MIS Research and Disciplinary Development', *Journal of Management Information Systems,* **8**(4), pp. 45-62.

Alfawaz, S., Nelson, K. and Mohannak, K. (2010). 'Information security culture: A behaviour compliance conceptual framework', *Proceedings of the Eighth Australasian Conference on Information Security-Volume* **105**, pp. 47-55.

Alnatheer, M. A. (2015). 'Information Security Culture Critical Success Factors', *Information Technology-New Generations (ITNG), 12th International Conference on Information Technology,* Las Vegas, April.

Altman, D., Burton, N. Cuthill, I. Festing, M. Hutton, J. and Playle, L. (2006). 'Why Do a Pilot Study', *National Centre for Replacement, Refinement and Reduction of Animal in Research,* **12**.

Amberg, M. Fischl, F. and Wiener, M. (2005). 'Background of Critical Success Factor Research', Friedrich-Alexander-Universitat Erlangen-Nurnberg Working.

Amid, A., Moalagh, M. and Ravasan, A. Z. (2012). 'Identification and Classification of ERP Critical Failure Factors in Iranian Industries', *Information Systems,* **37**(3), pp. 227-237.

Andrews, D., Nonnecke, B. and Preece, J. (2003). 'Electronic Survey Methodology: A Case Study in Reaching Hard-to-Involve Internet Users', *International Journal of Human-Computer Interaction,* **16**(2), pp. 185-210.

Angelakopoulos, G. and Mihiotis, A. (2011). 'E-banking: Challenges and Opportunities in the Greek Banking Sector', *Electronic Commerce Research,* **11**(3), pp. 297-319.

Aransiola, J. O. and Asindemade, S. O. (2011). 'Understanding Cybercrime Perpetrators and the Strategies They Employ in Nigeria', *Cyberpsychology, Behavior, and Social Networking,* **14**(12), pp. 759-763.

Archer, N. (2011). 'Consumer Identity Theft Prevention and Identity Fraud Detection Behaviours', *Journal of Financial Crime,* **19**(1), pp. 20-36.

Arend, M. (1993). 'New card fraud weapons emerge', *ABA Banking Journal,* **85**(9), p. 91.

Armitage, C. J. and Conner, M. (2001). ‘Efficacy of the Theory of Planned Behaviour: A Meta-Analytic Review’, *British Journal of Social Psychology,* **40**(4), pp. 471-499.

Armstrong, J.S. and Overton, T.S. (1977). ‘Estimating Nonresponse Bias in Mail Surveys’, *Journal of Marketing Research,* pp. 396-402.

Arnfield, R. (2014). ‘Preventing EMV Card Fraud by Using Real-Time Fraud-Detection Technology’. Available at: http://info.wincormarketing.co.uk/rs/wincornixdorf/images/Dynasty_WP_Preventing%20EMV%20Card%20Fraud%20by%20Using%20Real%20Time%20Fraud%20Detection%20Technology2.pdf

Arora, S. and Kaur, S. (2018). ‘Perceived Risk Dimensions & its Impact on Intension to Use E-baking Services: A Conceptual Study’, *Journal of Commerce & Accounting Research,* **7**(2).

Auta, E. M. (2010). ‘E-banking in Developing Economy: Empirical Evidence from Nigeria’, *Journal of Applied Quantitative Methods,* **5**(2).

Avison, D. E., Dwivedi, Y. K. Fitzgerald, G. and Powell, P. (2008). ‘The Beginnings of a New Era: Time to Reflect on 17 Years of the ISJ’, *Information Systems Journal,* **18**(1), pp. 5-21.

Ayo, C. K., Ekong, U. O. Afolabi, I. and Adebiyi, A. (2007). ‘M-commerce Implementation in Nigeria: Trends and Issues’, *Journal of Internet Banking and Commerce,* **12**(2).

Ayo, C. K. and Ukpere, W. I. (2010). ‘Design of a Secure Unified E-payment System in Nigeria: A Case Study’, *African Journal of Business Management,* **4**(9).

Ayres, L., Kavanaugh, K. and Knafl, K. A. (2003). ‘Within-case and Across-case Approaches to Qualitative Data Analysis’, *Qualitative Health Research,* **13**(6), pp. 871-883.

Aziz, N. M., and Salleh, H. (2011). ‘People Critical Success Factors of IT/IS Implementation: Malaysian Perspectives’, *World Academy of Science, Engineering and Technology,* **80**, pp. 75-82.

Babakus, E. and Mangold, W. G. (1992). ‘Adapting the SERVQUAL Scale to Hospital Services: An Empirical Investigation’, *Health Services Research,* **26**(6), pp. 767-786.

Bai, C. and Sarkis, J. (2013). ‘A Grey-Based DEMATEL Model for Evaluating Business Process Management Critical Success Factors’, *International Journal of Production Economics,* **146**(1), pp. 281-292.

Bai, X., Gopal, R. Nunez, M. and Zhdanov, D. (2012). ‘On the Prevention of Fraud and Privacy Exposure in Process Information Flow’, *INFORMS Journal on Computing,* **24**(3), pp. 416-432.

Baker, B. (1995). ‘The Role of Feedback in Assessing Information Systems Planning Effectiveness’, *The Journal of Strategic Information Systems,* **4**(1), pp. 61-80.

Balogun, S. K., Selemogwe, M. and Akinfala, F. (2013). ‘Fraud and Extravagant Life Styles Among Bank Employees: Case of Convicted Bank Workers in Nigeria’, *Psychological Thought,* **6**(2), pp. 252-263.

Barat, J. (1992). ‘Scenario Playing for Critical Success Factor Analysis’, *Journal of Information Technology,* **7**(1), pp. 12-19.

Barker, K. J., D'amato, J. and Sheridon, P. (2008). ‘Credit Card Fraud: Awareness and Prevention’, *Journal of Financial Crime,* **15**(4), pp. 398-410.

Bartlett, M. S. (1954). ‘A Note on the Multiplying Factors for Various χ^2 Approximations’, *Journal of the Royal Statistical Society.Series B (Methodological),* **16**(2), pp. 296-298.

Baxter, M. (1995). ‘Standardization and Transformation in Principal Component Analysis, with Applications to Archaeometry’, *Journal of the Royal Statistical Society. Series C (Applied Statistics),* **44**(4), pp. 513-527.

Bellovin, S. M. and Merritt, M. (1992). ‘Encrypted Key Exchange: Password-based Protocols Secure Against Dictionary Attacks’, *Research in Security and Privacy, Computer Society Symposium on Research in Security and Privacy,* California, May.

Benjamin, O. A.and Samson, B. S. (2011). ‘Effect of Perceived Inequality and Perceived Job Insecurity on Fraudulent Intent of Bank Employees in Nigeria’, *Europe’s Journal of Psychology,* **7**(1), pp. 99-111.

Bertram, D. (2007). ‘Likert Scales’. Available at: https://www.researchgate.net/profile/Zoi_Amprazi/post/what_is_a_logistic_regression_ana lysis/attachment/59d622fb79197b8077981515/AS:304626539139075@1449640034760/download/Likert+Scale+vs+Likert+Item.pdf.

Bharadwaj, S., Bhatt, H. S. Singh, R. Vatsa, M. and Noore, A. (2015). 'QFuse: Online Learning Framework for Adaptive Biometric System', *Pattern Recognition,* **48**(11), pp. 3428-3439.

Bhasin, M. L. (2015). 'Menace of Frauds in the Indian Banking Industry: An Empirical Study', *Australian Journal of Business and Management Research,* 4(12).

Bhasin, M. L. (2016). 'Integration of Technology to Combat Bank Frauds: Experience of a Developing Country', *Wulfenia Journal,* **23**(2), pp. 201-233.

Bhattacharyya, D., Ranjan, R. Alisherov, F. and Choi, M. (2009). 'Biometric Authentication: A review', *International Journal of u-and e-Service, Science and Technology,* **2**(3), pp. 13-28.

Bierstaker, J. L., Brody, R. G. and Pacini, C. (2006). 'Accountants Perceptions Regarding Fraud Detection and Prevention Methods', *Managerial Auditing Journal,* **21**(5), pp. 520-535.

Biometric Technology Today. (2016). 'IBM Adds Behavioural Biometrics to Banking Fraud Solution', *Biometric Technology Today,* (11), pp. 2-2.

Boardman, A., Greenberg, D. Vining, A. and Weimer, D. (1998). 'Cost-Benefit Analysis: Concepts and Practice (D. baracskay)', *Public Choice,* **96**(3), p. 417.

Bobbert, Y. and Mulder, H. (2015). 'Governance Practices and Critical Success Factors Suitable for Business Information Security'. International Conference on Computational Intelligence and Communication Networks, Jabalpur, December.

Booth, A., Sutton, A. and Papaioannou, D. (2016). *Systematic Approaches to a Successful Literature Review*. UK, London, Sage Publications.

Bouchard Jr, T. J. (1976). 'Unobtrusive Measures: An Inventory of Uses', *Sociological Methods and Research,* **4**(3), pp. 267-300.

Boynton, A. C. and Zmud, R. W. (1984). 'An Assessment of Critical Success Factors', *Sloan Management Review,* **25**(4), pp. 17-27.

Brereton, P., Kitchenham, B. A. Budgen, D. Turner, M. and Khalil, M. (2007). ‘Lessons from Applying the Systematic Literature Review Process within the Software Engineering Domain’, *Journal of Systems and Software,* **80**(4), pp. 571-583.

Browdie, B. (2012). ‘Bank of the West Installs Fraud Prevention Tool’, *American Banker,* **177**(154), p. 20-20.

Bruno, M. (2002). ‘UK Banks Eye Smart Cards’, *Bank Technology News,* **15**(10), p. 60.

Bryant, F. B. and Yarnold, P. R. (1995). ‘Principal-Components Analysis and Exploratory and Confirmatory Factor Analysis’, *In L. G. Grimm & P. R. Yarnold (Eds.), Reading and UnderstandingMmultivariate Statistics (pp. 99-136).* Washington, DC, US: American Psychological Association.

Budhram, T. (2014). ‘Lost, Stolen or Skimmed: Overcoming Credit Card Fraud in South Africa’, *South African Crime Quarterly,* **40**, pp. 31-37.

Bullen, C. V. and Rockart, J. F. (1981). ‘A Primer on Critical Success Factors’, Massachusetts Institute of Technology, Sloan School of Management, Massachusetts, USA.

Butler, T. and Fitzgerald, B. (1999). ‘Unpacking the Systems Development Process: An Empirical Application of the CSF Concept in a Research Context’, *The Journal of Strategic Information Systems,* **8**(4), pp. 351-371.

Butler, M. and Butler, R. (2015). ‘Investigating the Possibility to Use Differentiated Authentication Based on Risk Profiling to Secure Online Banking’, *Information and Computer Security,* **23**(4), pp. 421-434.

Camillo, M. (2017). ‘Cybersecurity: Risks and Management of Risks for Global Banks and Financial Institution’, *Journal of Risk Management in Financial Institutions,* **10**(2), pp. 196-200.

Caralli, R. A., Stevens, J. F. Willke, B. J. and Wilson, W. R. (2004). ‘The Critical Success Factor Method: Establishing a Foundation for Enterprise Security Management’, *Carnegie-Mellon Univ Pittsburgh Pa Software Engineering Inst.*

Card Technology Today. (2006). ‘Mag-stripe's the Problem!’, *Card Technology Today,* **18**(7–8), pp. 11-12.

Carlesi, G. (1981). ‘Cost/benefit Analyses of Information Systems’, *Management & Informatica,* **19**(9), pp. 559-561.

Carroll, J. M. and Swatman, P. A. (2000). ‘Structured-case: A Methodological Framework for Building Theory in Information Systems Research’, *European Journal of Information Systems*, **9**(4), pp. 235-242.

Cattell, R. B. (1966). ‘The Scree Test for the Number of Factors’, *Multivariate Behavioral Research*, **1**(2), pp. 245-276.

CBN. (2011). ‘Central Bank of Nigeria Annual Report, 2011’. Available at: https://www.cbn.gov.ng/documents/annualreports.asp

CBN. (2012). ‘National Financial Inclusion Strategy’. Available at: https://www.cbn.gov.ng/Out/2013/CCD/NFIS.pdf

CBN. (2013). ‘Central Bank of Nigeria Economic Report’. Available at: https://www.cbn.gov.ng/Out/2015/RSD/CBN%202013%20Annual%20Report.pdf

CBN. (2015a). ‘Safety Tips’. Available at: https://www.cbn.gov.ng/neff/safetytips.asp

CBN. (2015b). ‘Statement of CBN Core Mandate’. Available at: http://www.cbn.gov.ng/aboutcbn/Coremandate.asp

CBN. (2016a). ‘Monetary Policy Reforms’. Available at: http://www.cbn.gov.ng/monetaryPolicy/Reforms.asp

CBN. (2016b). ‘Cash-less Nigeria’. Available at: https://www.cbn.gov.ng/cashless/

CBN. (2017). ‘Guidelines on Operations of Electronic Payment Channels in Nigeria’. Available at: https://www.cbn.gov.ng/out/2016/bpsd/approved%20guidelines%20on%20operations%20of%20electronic%20payment%20channels%20in%20nigeria.pdf

Chang, S. J. Witteloostuijn, V. A., and Eden, L. (2010). ‘Common Method Variance in International Business Research’, *Journal of International Business Studies*, pp. 41-178.

Cheng, T. E., Lam, D. Y. and Yeung, A. C. (2006). ‘Adoption of Internet Banking: An Empirical Study in Hong Kong’, *Decision Support Systems*, **42**(3), pp. 1558-1572.

Choplin, J. M., Stark, D. P. and Ahmad, J. N. (2011). 'A psychological investigation of consumer vulnerability to fraud: Legal and policy implication', *35 law & psychol. rev. 61*.

Chow, T. and Cao, D. (2008). 'A Survey Study of Critical Success Factors in Agile Software Projects', *Journal of Systems and Software,* **81**(6), pp. 961-971.

Chua, C. E. H., Wareham, J. and Robey, D. (2007). 'The Role of Online Trading Communities in Managing Internet Auction Fraud', *MIS Quarterly,* **31**(4), pp. 759-781.

Clarke, N. L. and Furnell, S. M. (2007). 'Authenticating Mobile Phone Users Using Keystroke Analysis', *International Journal of Information Security,* **6**(1), pp. 1-14.

Cohen, J. (1988). *Statistical Power Analysis for the Behavioral Sciences 2nd edition*. Hillsdale, Erlbaum Associates.

Comrie, A. C. and Glenn, E. C. (1998). 'Principal Components-Based Regionalization of Precipitation Regimes Across the Southwest United States and Northern Mexico, with an Application to Monsoon Precipitation Variability*', Climate Research,* **10**(3), pp. 201-215.

Cone, B. D., Irvine, C. E.Thompson, M. F. and Nguyen, T. D. (2007). 'A Video Game for Cyber Security Training and Awareness', *Computers & Security,* **26**(1), pp. 63-72.

Coomber, R. (1997). 'Using the Internet for Survey Research', *Sociological Research Online,* **2**(2), pp.1-10.

Cooper, H. M. (1988). 'Organizing Knowledge Syntheses: A Taxonomy of Literature Reviews', *Knowledge in Society,* **1**(1), pp. 104-126.

Coram, P., Ferguson, C. and Moroney, R. (2008). 'Internal Audit, Alternative Internal Audit Structures and the Level of Misappropriation of Assets Fraud', *Accounting & Finance,* **48**(4), pp. 543-559.

Council, Federal Financial Institutions Examination. (2005). 'Authentication in an Internet Banking Environment'. Available at: https://www.ffiec.gov/%5C/pdf/authentication_guidance.pdf. Accessed: 18 *March* 2015.

Creswell, J. W. (2013). *Research design: Qualitative, Quantitative, and Mixed Methods Approaches.* UK, London, Sage Publications.

Creswell, J. W., Plano Clark, V. L. Gutmann, M. L. and Hanson, W. E. (2003). *Handbook of Mixed Methods in Social and Behavioral Research.*UK, London, Sage Publications.

Cronin, P., Ryan, F. and Coughlan, M. (2008). 'Undertaking a Literature Review: A step-by-step approach*', British Journal of Nursing*, **17**(1), pp. 38-43.

Crosman, P. (2017). 'Equifax Breach has Banks Tightening Defenses, Counseling Customers'. Available at: https://www.americanbanker.com/news/equifax-breach-has-banks-tightening-defenses-counseling-customers

Crossan, F. (2003). 'Research Philosophy: Towards an Understanding', *Nurse Researcher,* **11**(1), pp. 46-55.

Cummins, J. D., Lewis, C. M. and Wei, R. (2006). 'The Market Value Impact of Operational Loss Events for US Banks and Insurers', *Journal of Banking & Finance,* **30**(10), pp. 2605-2634.

Cunningham, J. A., Neighbors, C. Bertholet, N. and Hendershot, C. S. (2013). 'Use of Mobile Devices to Answer Online Surveys: Implications for Research'. Available at: https://bmcresnotes.biomedcentral.com/articles/10.1186/1756-0500-6-258

Dagogo, D. W. and Ngerebo, T. A. (2018). 'Bank Fraud and Financial Intermediation: A Supply-Side Causality Analysis', *Athens Journal of Business and Economics, **4**(1).*

Dalecki, M.G., Whitehead, J. C. and Blomquist, G. C. (1993). 'Sample Non-response Bias and Aggregate Benefits in Contingent Valuation: an Examination of Early, Late and Non-respondents', *Journal of Environmental Management,* **38**, pp. 133-143

Daszykowski, M., Kaczmarek, K. Vander Heyden, Y. and Walczak, B. (2007). 'Robust Statistics in Data Analysis - a Review: Basic Concepts*', Chemometrics and Intelligent Laboratory Systems, **8***5(2), pp. 203-219.

Datta, S. K. (2010). 'Acceptance of E-banking Among Adult Customers: An Empirical Investigation in India', *Journal of Internet Banking and Commerce,* **15**(2), p. 1.

Davenport, E. C., Davison, M. L. Liou, P. and Love, Q. U. (2015). 'Reliability, Dimensionality, and Internal Consistency as Defined by Cronbach: Distinct Albeit Related Concepts*', Educational Measurement: Issues and Practice, **34***(4), p. 4-9.

Daw, D. (2012). 'The Growing Threat of ATM Skimmer Scams', *PC World,* **30**(3), pp. 35-36.

Dawes, J. (2008). ‘Do Data Characteristics Change According to the Number of Scale Points Used’, *International Journal of Market Research,* **50**(1), p. 61-77.

De Sousa, José Manuel Esteves. (2004). ‘Definition and Analysis of Critical Success Factors for ERP Implementation Projects’, unpublished Ph.D thesis, University of Catalonia, Spain.

DeCoster, J. (1998). ‘Overview of Factor Analysis’. Available at: http://www.stat-help.com/notes.html. Accessed: 7 July 2018.

Della-Libera, G., Dixon, B. Farrell, J. Garg, P. Hondo, M. Kaler, C. and Leach, P. (2002). ‘Security in a Web Services World: A Proposed Architecture and Roadmap’, *Online Whitepaper, IBM Corporation and Microsoft Corporation,* p.7.

Dictionary, O. E. (2007). ‘Oxford English Dictionary Online’. Available at: https://qhylrusmp.updog.co/cWh5bHJ1c21wMDE5ODYwNTc1Nw.pdf

Dimitriadis, C. K. and Shaikh, S. A. (2007). ‘A Biometric Authentication Protocol for 3G Mobile Systems: Modelled and Validated Using CSP and Rank Functions’, *International Journal of Network Security,* **5**(1), pp. 99-111.

Dolnicar, S. (2013). ‘Asking Good Survey Questions’, *Journal of Travel Research,* **52**(5), pp. 551-574.

Dong, Y. and Peng, C. J. (2013). ‘Principled Missing Data Methods for Researchers*’,* *SpringerPlus,* **2**(1), p. 222.

Dooley, L. M. (2002). ‘Case Study Research and Theory Building’, *Advances in Developing Human Resources,* **4**(3), pp. 335-354.

Dunteman, G.H. (1989). *Principal Components Analysis.* USA, California, Sage Publications.

Dwyer, S., Hill, J. and Martin, W. (2000). ‘An Empirical Investigation of Critical Success Factors in the Personal Selling Process for Homogenous Goods’, *Journal of Personal Selling & Sales Management,* **20**(3), pp. 151-159.

Dzemydeine, D., Naujikiene, R. Kalinauskas, M. and Jasiunas, E. (2010). ‘Evaluation of Security Disturbance Risks in Electronic Financial Payment Systems’, *Intellectual economics,* **2** (8).

Economist. (2014). ‘Credit cards: Skimming off the Top’, *Economist,* **410**, pp. 53-53.

Efiong, E. J., Inyang, I. O. and Joshua, U. (2016). ‘Effectiveness of the Mechanisms of Fraud Prevention and Detection in Nigeria’, *Advances in Social Sciences Research Journal,* **3**(3).

Eisenhardt, K. M. (1989). ‘Building Theories from Case Study Research’, *Academy of Management Review,* **14**(4), pp. 532-550.

Efiong, E. J., Inyang, I. O. and Joshua, U. (2016). ‘Effectiveness of the Mechanisms of Fraud Prevention and Detection in Nigeria’, *Advances in Social Sciences Research Journal,* **3**(3).

Enofe, A., Abilogun, T. Omoolorun, A. and Elaiho, E. (2017). ‘Bank Fraud and Preventive Measures in Nigeria: An Empirical Review’, *International Journal of Academic Research in Business and Social Sciences,* **7**(7), pp. 40-51.

Epstein, M. J. (2004). *Implementing E-commerce Strategies: A guide to Corporate Success After the Dot. Com Bust.* Westport, Greenwood Publishing Group.

Epstein, J. D. (2017). ‘The Government's Golden Rule: America's Attempts to Control Health Care Payment’, *Journal of Health & Life Sciences Law,* **10**(3), pp. 34-65.

Ernest Chang, S. and Ho, C. B. (2006). ‘Organizational Factors to the Effectiveness of Implementing Information Security Management’, *Industrial Management & Data Systems,* **106**(3), pp. 345-361.

Esteves, J. and Pastor, J. (2004). ‘Using a Multimethod Approach to Research Enterprise Systems Implementations’, *Electronic Journal of Business Research Methods,* **2**(2), pp. 69-82.

Etchegaray, J. M. and Fischer, W. G. (2010). ‘Understanding Evidence-Based Research Methods: Reliability and Validity Considerations in Survey Research’, *Herd,* **4**(1), pp. 131-135.

Ewusi-Mensah, K. (1989). ‘Evaluating Information Systems Projects: A Perspective on Cost-benefit Analysis’, *Information Systems,* **14**(3), pp. 205-217.

EY. (2016). ‘14th global fraud survey 2016’. Available at: http://www.ey.com/Publication/vwLUAssets/EY-14-global-fraud-survey/$FILE/EY-14-global-fraud-survey.pdf

Falola, T., Genova, A. and Heaton, M. M. (2018). ‘Historical Dictionary of Nigeria’, **2**, pp. 2-314. Rowman & Littlefield.

Feldman, M. A. (2011). ‘Key Performance Indicators: Developing, Implementing, and Using Winning KPIs’, *Quality Progress,* **44**(9), pp. 68-69.

Financial Fraud Action. (2010). ‘Fraud the Facts’. Available at: http:www.Financialfraudaction.Org.uk/download.asp.

Financial Fraud Action. (2016). ‘Fraud the Facts 2016 the Definitive Overview of Payment Industry Fraud and Measures to Prevent It’. Available at: https://www.financialfraudaction.org.uk/fraudfacts17/assets/fraud_the_facts.pdf;

Financial Times. (2017). ‘UK Card Fraud Falls After Banks Tighten Security’. Available at: https://www.ft.com/content/fe2a6a88-a451-11e7-9e4f-7f5e6a7c98a2

Finfgeld-Connett, D. and Johnson, E. D. (2013). ‘Literature Search Strategies for Conducting Knowledge-building and Theory-generating Qualitative Systematic Reviews’, *Journal of Advanced Nursing,* **69**(1), pp. 194-204.

Fischer, F. (2003). ‘Policy Analysis as Discursive Practice: The Argumentative Turn’, *Reframing Public Policy Discursive Politics and Deliberative Practices,* pp. 181-202.

Fishman, L. N., Barendse, R. M. Hait, E. Burdick, C. and Arnold, J. (2010). ‘Self-management of Older Adolescents with Inflammatory Bowel Disease: A Pilot Study of Behavior and Knowledge as Prelude to Transition’, *Clinical Pediatrics,* **49**(12), pp. 1129-1133.

Flynn, D. J. and Arce, E. A. (1997). ‘A CASE Tool to Support Critical Success Factors Analysis in IT Planning and Requirements Determination’, *Information and Software Technology,* **39**(5), pp. 311-321.

Foon, Y. S. and Fah, B. C. Y. (2011). ‘Internet Banking Adoption in Kuala Lumpur: An Application of UTAUT Model’, *International Journal of Business and Management,* **6**(4), p. 161.

Foster, D., Matton, N. and Walker, P. (2009). ‘Using Multiple Online Security Measures to Deliver Secure Course Exams to Distance Education Students’, Accessed: 10 June 2012.

Foster, S., Lazarenko, K. Hawking, P. and Stein, A. (2007). ‘A Change Strategy for Organisational Security the Role of Critical Success Factors’. In Proceedings of the Ninth International Conference on Enterprise Information Systems, Madeira, June.

Frazier, D. and Rohmund, I. (2007). ‘The Real-time Benefits of Online Surveys’, *Electric Perspectives,* **32**(4), pp. 88-91.

French, A. M. (2012). ‘A Case Study on E-banking Security-when Security Becomes too Sophisticated for the User to Access their Information’, *Journal of Internet Banking and Commerce,* **17**(2), pp. 1-14.

Fukuda, H. and Ohashi, Y. (1997). ‘A Guideline for Reporting Results of Statistical Analysis in Japanese Journal of Clinical Oncology*', Japanese Journal of Clinical Oncology,* **27**(3), pp. 121-127.

Furnell, S. and Vasileiou, I. (2017). ‘Security Education and Awareness: Just Let them Burn?’, *Network Security, 2017,* (12), pp. 5-9.

Ganesan, R. and Vivekanandan, K. (2009). ‘A Novel Hybrid Security Model for E-commerce Channel’. Advances in Recent Technologies in Communication and Computing (pp. 293-296), International Conference, Kerala, October.

Gao, W. and Kim, J. (2007). ‘Robbing the Cradle is Like Taking Candy from a Baby’. Proceedings of the Annual Conference of the Security Policy Institute (GCSPI*)*, pp. 23-37.

Gar, K. K. (2014). ‘Critical Success Factors of Project Management for Dam Construction Projects in Myanmar’, unpublished Ph.D thesis, BRAC institute of Governance and Development of BRAC University.

Gates, T. and Jacob, K. (2009). ‘Payments Fraud: Perception Versus Reality - A Conference Summary’, *Economic Perspectives,* **33**(1), pp. 7-15.

George, A. L. and Bennett, A. (2005) *Case Studies and Theory Development in the Social Sciences*. Cambridge, MIT Press.

George, D. and Mallery, M. (2003). *Using SPSS for Windows Step by Step: A Simple Guide and Reference*. Boston: Allyn & Bacon, pp.222-232.

Gercke, M. (2007). 'Internet-related Identity Theft'. Available at: https://www.coe.int/t/DG1/LEGALCOOPERATION/ECONOMICCRIME/cybercrime/cy%20activity_events_on_identity_theft/567%20port%20id-d-identity%20theft%20paper%2022%20nov%2007.pdf

Gersick, C. J. (1988). 'Time and Transition in Work Teams: Toward a New Model of Group Development', *Academy of Management Journal,* **31**(1), pp. 9-41.

Giles, J. (2010). 'The Problem with Online Banking', *New Scientist,* **205**(2745), pp. 18-19.

Glaser, B. and Strauss, A. (1967). 'The Discovery of Grounded Theory', *London: Weidenfeld and Nicholson,* **24**(25), pp. 288-304.

Glasow, P. A. (2005). *Fundamentals of Survey Research Methodology*. Virginia, MITTRE.

Glass, N. M. and Schmidt, M. (1991). *Pro-active Management: How to improve your management performance*. East Brunswick, NJ: Nichols

Gliem, R. R. and Gliem, J. A. (2003). 'Calculating, Interpreting, and Reporting Cronbach's Alpha Reliability Coefficient for Likert-type Scales'. Midwest Research-to-Practice Conference in Adult, Continuing, and Community Education, Ohio, October.

Goi, C. L. (2006). 'Factors Influence Development of E-banking in Malaysia', *Journal of Internet Banking and Commerce,* **11**(2), pp. 1-21.

Golafshani, N. (2003). 'Understanding Reliability and Validity in Qualitative Research', *The Qualitative Report,* **8**(4), pp. 597-606.

Goldstein, D. K. and Rockart, J. F. (1984). 'An Examination of Work-Related Correlates of Job Satisfaction in Programmer/analysts', *MIS Quarterly,* pp. 103-115.

Grace, E., Rai, A. Redmiles, E. Ghani, R. Joshi, J. Karypis, G. and Suzumura, T. (2016). 'Detecting Fraud, Corruption, and Collusion in International Development Contracts: The Design of a Proof-of-Concept Automated System'. In Big Data 2016 IEEE International Conference on, pp. 1444-1453.

Greene, J. C. and Caracelli, V. J. (1997). *Advances in Mixed-method Evaluation: The Challenges and Benefits of Integrating Diverse Paradigms.* San Francisco, Jossey-Bass Publishers.

Griffith, E. (2010). 'Password Protection: How to Create Strong Passwords', *PC Magazine,* **29**(10), pp. 1-1.

Grunert, K. G. and Ellegaard, C. (1992). *The Concept of Key Success Factors: Theory and Method.* MAPP.

Guba, E. G., and Lincoln, Y. S. (1994). 'Competing Paradigms in Qualitative Research', *Handbook of Qualitative Research,* **2**(163-194), p. 105.

Hair, J. F., Black, W. C., Babin, B. J. Anderson, R. E. and Tatham, R. L. (2006). *Multivariate Data Analysis 6th Edition*. New Jersey: Pearson Education.

Hamidi, N. A., Rahimi, G. M. Nafarieh, A. Hamidi, A. and Robertson, B. (2013). 'Personalized Security Approaches in E-banking Employing Flask Architecture Over Cloud Environment', *Procedia Computer Science,* **21**, pp. 18-24.

Haque, A., Ismail, A. Z. and Daraz, A. H. (2009). 'Issues of E-banking Transaction: An Empirical Investigation on Malaysian Customers Perception', *Journal of Applied Sciences,* **9**(10), pp. 1870-1879.

Hart, C. (1998). *Doing a Literature Review: Releasing the Social Science Research Imagination.* London, Sage Publications.

Henderson, J. C., Rockart, J. F. and Sifonis, J. G. (1984). 'A Planning Methodology for Integrating Management Support Systems'. Available at: https://dspace.mit.edu/bitstream/handle/1721.1/2090/SWP-1591-12173714-CISR-116.pdf

Henning, J. E., Stone, J. M. and Kelly, J. L. (2009). *Using Action Research to Improve Instruction: An Interactive Guide for Teachers*, Routledge.

Herley, C. and Van Oorschot, P. (2012). 'A Research Agenda Acknowledging the Persistence of Passwords', *IEEE Security & Privacy,* **10**(1), pp. 28-36.

Hertzum, M., Jørgensen, N. and Nørgaard, M. (2004). 'Usable Security and E-banking: Ease of Use Vis-a-vis Security', *Australasian Journal of Information Systems,* **11**(2).

Hinson, G. (2003). 'Human Factors in Information Security'. *Procedia - Social and Behavioral Sciences*, 147

Hirschheim, R., Klein, H. K. and Lyytinen, K. (1996). 'Exploring the Intellectual Structures of Information Systems Development: A Social Action Theoretic Analysis', *Accounting, Management and Information Technologies,* **6**(1), pp. 1-64.

Ho, L. and Lin, G. (2004). 'Critical Success Factor Framework for the Implementation of Integrated-Enterprise Systems in the Manufacturing Environment', *International Journal of Production Research,* **42**(17), pp. 3731-3742.

Hogan, T. P., Benjamin, A. and Brezinski, K. L. (2000). 'Reliability Methods: A Note on the Frequency of Use of Various Types', *Educational and Psychological Measurement,* **60**(4), pp. 523-531.

Holden, M. T. and Lynch, P. (2004). 'Choosing the Appropriate Methodology: Understanding Research Philosophy', *The Marketing Review,* **4**(4), pp. 397-409.

Holzenthal, F. (2017). 'Five Trends Shaping the Fight Against Financial Crime', *Computer Fraud & Security,* **2017**(3), pp. 5-9.

Hong, K., Chi, Y. Chao, L. R. and Tang, J. (2003). 'An Integrated System Theory of Information Security Management', *Information Management & Computer Security,* **11**(5), pp. 243-248.

Hopkins, P. (2011). 'Internet Fraud: 10 Best Strategies for Protecting your Banking Website', *Illinois Banker,* **96**(11), pp. 10-13.

Hosseini, S. S. and Mohammadi, S. (2012). 'Review Banking on Biometric in the World's Banks and Introducing a Biometric Model for Iran's Banking System', *Journal of Basic and Applied Scientific Research,* **2**(9), pp. 9152-9160.

Hoza, B. and WÓJCICKI, M. (2017). 'Vat Fraud Prevention', *Zeszyty Naukowe* , (2), pp. 44-58.

Hulsebosch, R., Giinther, C. Horn, G. Holtmanns, S. Howker, K. Paterson, K. and Mitchell, C. J. (2004). *Pioneering Advanced MobilePrivacy and Security.* C. J. Mitchell (Ed.): Stevenage, UK.

Humphrey, S. (2017). 'Identifying the Critical Success Factors to Improve Information Security Incident Reporting', unpublished Ph.D thesis, Cranfield University.

Hurley, A.E., Scandura, T.A., Schriesheim, C.A., Brannick, M.T., Seers, A., Vandenberg, R.J. and Williams, L.J., (1997). 'Exploratory and confirmatory factor analysis: Guidelines, issues, and alternatives', *Journal of Organizational Behavior: The International Journal of Industrial,* **18**(6), pp. 667-683.

Hwang, M. (2003). 'Critical Success Factors for Data Warehouse Implementation: A Framework for Analysis and Research', *Information Technology and Organizations: Trends, Issues, Challenges and Solutions,* **1**, p. 195.

Hyman, J. P. (1985). 'New Card Security Measures Can Help Banks Beat Fraud', *Bank Systems & Equipment,* **22**(4), pp. 40-41.

Iarossi, G. (2006). *The Power of Survey Design: A User's Guide for Managing Surveys, Interpreting Results, and Influencing Respondents*. World Bank Publications.

Idolor, E. J. (2010). 'Bank Frauds in Nigeria: Underlying Causes, Effects and Possible Remedies', *African Journal of Accounting, Economics, Finance and Banking Research,* **6**(6), p. 62.

Igwe, C. N. (2011). 'Socio-Economic Developments and the Rise of 419 Advanced-fee Fraud in Nigeria', *European Journal of Social Science,* **20**(1), pp. 184-193.

Imroz, S. M. (2009). 'Application of Q-Methodology in Critical Success Factors of Information Security Risk Management', unpublished MS.c thesis, University of Nebraska at Omaha.

Israel, M. and Hay, I. (2006). *Research Ethics for Social Scientists,* pp. 51-52. UK, London, Sage Publications.

Jackson, J.E. (2005). *A User's Guide to Principal Components.* USA, New York, John Wiley & Sons.

Jain, A. K., Ross, A. and Pankanti, S. (2006). 'Biometrics: A Tool for Information Security', *IEEE Transactions on Information Forensics and Security,* **1**(2), pp. 125-143.

Jalonen, H. and Lönnqvist, A. (2011). 'Exploring the Critical Success Factors for Developing and Implementing A Predictive Capability in Business', *Knowledge & Process Management,* **18**(4), pp. 207-219.

Jankowicz, A. (2000). *Business Research Methods.* Press, Plano, TX.

Jankowicz, A.D. (2005). *Business Research Projects: 4th Edition*. Cengage Learning, UK, London, Thomson.

Javadin, S. R. S., Raei, R. Iravani, M. J. and Safari, M. (2015). 'Conceptualizing and Examining the Critical Success Factors for Implementing Islamic Banking System Towards Banking Sector of Iran: A Mixed Method Approach', *Iranian Journal of Management Studies,* **8**(3), p. 421.

Javelin. (2017). 'Identity Fraud Hits Record High With 15.4 million U.S. Victims in 2016, up 16 percent According to New Javelin Strategy & Research Study'. Available at: https://www.javelinstrategy.com/press-release/identity-fraud-hits-record-high-154-million-us-victims-2016-16-percent-according-new

Jick, T.D. (1979). 'Mixing Qualitative and Quantitative Methods: Triangulation in Action', *Administrative Science Quarterly,* **24**(4), pp. 602-611.

Jin, N. and Fei-Cheng, M. (2005). 'Network Security Risks in Online Banking', *Wireless Communications, Networking and Mobile Computing,* 2, pp. 1229-1234.

Johns, R. (2010). 'Likert Items and Scales', *Survey Question Bank: Methods Fact Sheet,* **1**, pp. 1-11.

Johnson, M. and Moore, S. (2007). 'A New Approach to E-banking'. Nordic Conference on Secure IT Systems, Copenhagen, October.

Johnson, R. B. and Onwuegbuzie, A. J. (2004). 'Mixed Methods Research: A Research Paradigm Whose Time Has Come', *Educational Researcher,* **33**(7), pp. 14-26.

Johnson, R.B., Onwuegbuzie, A.J. and Turner, L.A. (2007). 'Toward a Definition of Mixed Methods Research', *Journal of Mixed Methods Research,* **1**(2), pp. 112-133.

Jolliffe, I. T. (2002). *Principal Component Analysis and Factor Analysis.* Springer Series in Statistics, New York, Springer.

Joliffe, I.T. and Morgan, B.J.T. (1992). 'Principal Component Analysis and Exploratory Factor Analysis', *Statistical Methods in Medical Research,* **1**(1), pp. 69-95.

Joslin, R. and Müller, R. (2016). ‘Identifying Interesting project Phenomena Using Philosophical and Methodological Triangulation’, *International Journal of Project Management,* **34**(6), pp. 1043-1056.

Kaiser, M. (1974). ‘Kaiser-meyer-olkin Measure for Identity Correlation Matrix’, *Journal of the Royal Statistical Society,* **52**.

Kajornboon, A. B. (2005). ‘Using Interviews as Research Instruments’, *E-Journal for Research Teachers,* **2**(1), pp. 1-9.

Kamel, S. (2006). *Electronic Business in Developing Countries: Opportunities and Challenges.* IGI Global.

Kaplan, B. and Duchon, D. (1988). ‘Combining Qualitative and Quantitative Methods in Information Systems Research: A Case Study’, *MIS Quarterly,* pp. 571-586.

Karamala, P. and Anchula, B. D. (2011). ‘Does an ATM Surrogate a Branch of a Bank in India?’, *Journal of Business and Retail Management Research,* **6**(1).

Kavitha, S. (2017). ‘Factors Influencing Satisfaction on E-banking’, *AIMS International Journal of Management,* **11**(2), pp. 103-115.

Keely, D. (2001). *A Security Strategy for Mobile E-business.* Tech.Rep. GSOEE213. IBM Global Services

Kelle, U. (2006). ‘Combining Qualitative and Quantitative Methods in Research Practice: Purposes and Advantages’, *Qualitative Research in Psychology,* **3**(4), pp. 293-311.

Kerlinger, F. and Lee, H. (2000). ‘Validity’, *Foundations of Behavioral Research.4th Ed.BelmontCA: Cengage,* pp. 665-688.

Khan, M. S. and Mahapatra, S. S. (2009). ‘Service Quality Evaluation in Internet Banking: An Empirical Study in India’, *International Journal of Indian Culture and Business Management,* **2**(1).

Khandelwal, V. K. and Ferguson, J. R. (1999). ‘Critical Success Factors (CSF) and the Growth of IT in Selected Geographic Regions’. Proceedings of the 32nd Annual Hawaii International Conference on, pp. 13-pp. IEEE, 1999.

Khazanchi, D. and Munkvold, B. E. (2003). ‘On the Rhetoric and Relevance of IS Research Paradigms: A Conceptual Framework and Some Propositions’. In Proceedings of the 36th Annual Hawaii International Conference on, pp. 10-pp. IEEE, 2003.

Kitchenham, B. (2004). Procedures For Performing Systematic Reviews’, *Keele University,* **33**, pp. 1-26.

Klein, H. K. and Myers, M. D. (1999). ‘A Set of Principles for Conducting and Evaluating Interpretive Field Studies in Information Systems’, *MIS Quarterly,* pp. 67-93.

Koskosas, I. (2011). ‘E-banking Security: A Communication Perspective’, *Risk Management,* **13**(1-2), pp. 81-99.

Kothari, C. R. (2004). *Research Methodology: Methods and Techniques*. New Delhi, New Age International.

KPMG. (2017). ‘How Can Nigerian Banks Start to Improve Internet Banking Penetration?’. Available at: https://home.kpmg.com/ng/en/home/insights/2017/11/how-can-nigerian-banks-start-to-improve-internet-banking-penetra.html

Krishnan, J. M. (2017). ‘Customers Attitude Towards E-banking System in Chennai’, *International Journal of Research in Management & Social Science,* **5**(3), p. 68.

Krummeck, S. (2000). ‘The Role of Ethics in Fraud Prevention: A Practitioner’s Perspective’, *Business Ethics: A European Review,* **9**(4), pp. 268-272.

Kryukov, D. and Strauss, R. (2009). ‘Information Security Governance as Key Performance Indicator for Financial Institutions’, *The Journal of Riga Tecjnocal University,* **38**, pp. 161-167.

Kumar, A. and Gupta, H. (2009). ‘Branchless Banking and Financial Inclusion’, *Siliconindia,* **12**(8), pp. 40-42.

Kurttila, M., Pesonen, M. Kangas, J. and Kajanus, M. (2000). ‘Utilizing the Analytic Hierarchy Process (AHP) in SWOT Analysis — a Hybrid Method and its Application to a Forest-Certification Case’, *Forest Policy and Economics,* **1**(1), pp. 41-52.

Lallmahamood, M. (2007). ‘An Examination of Individual's Perceived Security and Privacy of the Internet in Malaysia and the Influence of this on their Intention to Use E-commerce:

Using an Extension of the Technology Acceptance Model', *Journal of Internet Banking and Commerce,* **12**(3), p. 1.

Lamont, J. (2010). 'Real-Time Fraud Countermeasures', *KM World,* **19**(7), pp. 12-21.

Leedy, P. and Ormrod, J. (2010). *Practical Research Planning and Design*. 9th edition Boston: Pearson Education International.

Leidecker, J. K. and Bruno, A. V. (1984). 'Identifying and Using Critical Success Factors', *Long Range Planning,* **17**(1), pp. 23-32.

Lemos, R. (2006). 'Password Policies', *PC Magazine,* **25**(8), pp. 116-116.

Li, J. (2008). 'Ethical Challenges in Participant Observation: A Reflection on Ethnographic Fieldwork', *The Qualitative Report,* **13**(1), pp. 100-115.

Lin, I. and Schaeffer, N. (1995). 'Using Survey Participants to Estimate the Impact of Nonparticipation.', *The Public Opinion Quarterly,* **59**(2), pp. 236-258.

Lincoln, T. (1990). *Managing Information Systems for Profit.* New York, USA, Wiley & Sons, Inc, pp. 103-146.

Lincoln, Y. S. and Guba, E. G. (1985). *Naturalistic Inquiry.* California, Sage Publications.

Lopes, I. M. and Oliveira, P. (2015). 'Critical Success Factors for the Implementation of a Security Policy in Health Clinics', *Information Systems and Technologies (CISTI),* pp. 1-7.

Lynham, S. A. (2000). 'Theory Building in the Human Resource Development Profession', *Human Resource Development Quarterly,* **11**(2), p. 159.

Maçada, A. C. G. and Luciano, E. M. (2010). 'The Influence of Human Factors on Vulnerability to Information Security Breaches'. Americas Conference on Information Systems, Lima, August

Madhok, A., Madhok, C. and Sethi, P. (2002). *System and Method for Detecting Card Fraud*. U.S. Patent Application 10/510,277.

Mahdi, M. D. H., Rezaul, K. M. Rahman, M. A. Berntzen, L. Bodendorf, F. Lawrence, E. and Smedberg, A. (2010). ‘Credit Fraud Detection in the Banking Sector in UK: A Focus on E-business’, *In Digital Society*, pp. 232-237.

Mahony, C. (2014). ‘Should Precipitation Variables be Transformed Prior to PCA?’. Available at: http://blogs.ubc.ca/colinmahony/2014/10/17/should-precipitation-variables-be-transformed-prior-to-pca/

Makarevic, N. (2015). ‘Comparative Analysis of Perceptions Towards IT Security in Online Banking: Serbian Clients vs. Clients of Bosnia and Herzegovina’, *Journal of Business Studies Quarterly,* **7**(2), pp. 242-257.

Malek, W. W. Z., Mayes, K. and Markantonakis, C. (2008). ‘Fraud Detection and Prevention in Smart Card Based Environments Using Artificial Intelligence’. International Conference on Smart Card Research and Advanced Applications, London, September.

Malhotra, M. K. and Grover, V. (1998). ‘An Assessment of Survey Research in POM: From Constructs to Theory*’, Journal of Operations Management,* **16**(4), pp. 407-425.

Mannan, M. and van Oorschot, P. C. (2011). ‘Leveraging Personal Devices for Stronger Password Authentication from Untrusted Computers’, *Journal of Computer Security,* **19**(4), pp. 703-750.

MarketLine. (2012). *Lloyds Banking Group plc SWOT Analysis*. Lloyds TSB Group, PLC SWOT Analysis, pp. 1-8.

Masocha, R., Chiliya, N. and Zindiye, S. (2011). ‘E-banking Adoption by Customers in the Rural Milieus of South Africa: A Case of Alice, Eastern Cape, South Africa’, *African Journal of Business Management,* **5**(5), p. 1857.

Matthew, K., Patrick, K. and Denise, K. (2013). ‘The Effects of Fraudulent Procurement Practices on Public Procurement Performance’, *International Journal of Business and Behavioral Sciences,* **3**(1), pp. 17-27.

McAteer, M. J. (2009). *Indicators of Management Fraud in Community Banks.* The Analytic Model of Management Fraud.

Menga, E., Dan, A. Lu, J. and Liu, X. (2015). ‘Ranking Alternative Strategies by SWOT Analysis in the Framework of the Axiomatic Fuzzy Set Theory and the ER Approach’, *Journal of Intelligent & Fuzzy Systems,* **28**(4), pp. 1775-1784.

Mertens, D. M. and Hesse-Biber, S. (2012). ‘Triangulation and Mixed Methods Research: Provocative Positions’, *Journal of Mixed Methods Research,* **6**(2), pp. 75-79.

Micheni, E. M. (2017). ‘Analysis of the Critical Success Factors of Integrated Financial Management Information Systems in Selected Kenyan Counties’, *Journal of Finance and Accounting,* **5**(5), 185.

Mihalcescu, C., Ciolacu, B. Pavel, F. and Titrade, C. (2008). ‘Risk and Inovation in E-banking’, *Romanian Economic and Business Review,* **3**(2), p. 86.

Miles, M. B. and Huberman, A. M. (1994). *Qualitative Data Analysis: An Expanded Sourcebook.* Los Angeles, Sage Publications.

Miranda, P., Isaias, P. Costa, C. J. Zaphiris, P. and Ioannou, A. I. (2014). ‘From Information Systems to E-learning 3.0 Systems's Critical Success Factors: A Framework Proposal’. International Conference on Learning and Collaboration Technologies, pp. 180-191.

Mishra, R. P. and Chakraborty, A. (2014). ‘Strengths, Weaknesses, Opportunities and Threats Analysis of Lean Implementation Frameworks’, *International Journal of Lean Enterprise Research,* **1**(2), pp. 162-182.

Mohammed, L. A. (2018). ‘ATM Frauds-Preventive Measures and Cost Benefit’, *GSTF Journal on Computing,* **1**(2).

Mohd-Sanusi, Z., Rameli, M. Omar, N. and Ozawa, M. (2015). ‘Governance Mechanisms in the Malaysian Banking Sector: Mitigation of Fraud Occurrence’, *Asian Journal of Criminology,* ***10***(3), pp. 231-249.

Monica, P. (2014). ‘An Approach to Fraud Risk Management’, *SEA-Practical Application of Science,* (5), pp. 67-74.

Monrose, F. and Rubin, A. D. (2000). ‘Keystroke Dynamics as a Biometric for Authentication’, *Future Generation Computer Systems,* **16**(4), pp. 351-359.

Moore, T., Clayton, R. and Anderson, R. (2009). 'The Economics of Online Crime', *The Journal of Economic Perspectives,* **23**(3), pp. 3-20.

Moskovitch, R., Feher, C. Messerman, A. Kirschnick, N. Mustafić, T. Camtepe, A. and Rokach, L. (2009). 'Identity Theft, Computers and Behavioral Biometrics'. International Conference on Intelligence and Security Informatics, Dallas, June.

Mouton, J. (1996). *Understanding Social Research.* Hatfield, Van Schaik Publishers.

Mulrow, C.D. (1994). 'Systematic Reviews: Rationale for Systematic Reviews', *Bmi,* **309**(6954), pp. 597-599.

Murdoch, S. J. and Anderson, R. (2010). 'Verified by Visa and Mastercard Securecode: Or, How Not to Design Authentication'. International Conference on Financial Cryptography and Data Security, Tenerife, January.

Mutunga, J. N. (2013). 'Operational Challenges in the Implementation of E-banking at the National Bank of Kenya', unpublished MBA thesis: Faculty of Business Administration, University of Nairobi.

Myyry, L., Siponen, M. Pahnila, S. Vartiainen, T. and Vance, A. (2009). 'What Levels of Moral Reasoning and Values Explain Adherence to Information Security Rules? An Empirical Study', *European Journal of Information Systems,* **18**(2), pp. 126-139.

National Mortgage News. (2006). 'Flagstar Automates Fraud Detection', *National Mortgage News,* **30**(44), pp. 25-25.

Neale, P., Thapa, S. and Boyce, C. (2006). *Preparing a Case Study: A Guide for Designing and Conducting a Case Study for Evaluation Input.* Pathfinder International Massachusetts.

NeFF. (2017). 'The Nigeria Electronic Fraud Forum Annual Report, 2016'. Available at: Https://www.Cbn.Gov.ng/Out/2017/CCD/A%20CHANGING%20PAYMENTS%20ECOSYSTEM%20NeFF%202016%20Annual%20Report.Pdf.

Neuman, W. L. (2005). *Social Research Methods: Quantitative and Qualitative Approaches.* Allyn and bacon Boston, MA.

Newman, G. and McNally, M. M. (2005). *Identity Theft Literature Review.* Citeseer.

Nilson. (2016). *Card Fraud Losses Reach $21.94 billion.* The Nilson Report, Nilson.

Newman, I. and Benz, C. R. (1998). *Qualitative-Quantitative Research Methodology: Exploring the Interactive Continuum.* SIU Press.

Ngai, E. W., Law, C. C. and Wat, F. K. (2008). 'Examining the Critical Success Factors in the Adoption of Enterprise Resource Planning', *Computers in Industry,* **59**(6), pp. 548-564.

Niranjanamurthy, M. and Chahar, D. D. (2013). 'The Study of E-commerce Security Issues and Solutions', *International Journal of Advanced Research in Computer and Communication Engineering,* **2**(7).

Norman K. Denzin and Yvonna S. Lincoln. (2005). *The Sage Handbook of Qualitative Research.* Sage Publications.

Nortman, D. L., Halvas, J. and Rabago, A. (1986). 'A Cost-Benefit Analysis of the Mexican Social Security Administration's Family Planning Program', *Studies in Family Planning,* **17**(1), pp. 1-6.

Novikov, A.M. and Novikov, D.A. (2013). *Research Methodology: From Philosophy of Science to Research Design.* US, Boca Raton, CRC Press.

Nyandoro, A. and Mahleko, B. (2015). 'A SWOT Analysis of Mobile Electronic Banking: The Zimbabwe Case', *International Journal of Electronic Finance,* **8**(2), pp. 218-238.

Obstfeld, M. and Rogoff, K. (2009). 'Global Imbalances and the Financial Crisis: Products of Common Causes'. CEPR Discussion Paper No. DP7606. Available at: https://ssrn.com/abstract=1533211

Ogbalu, M. (2016). 'Achieving SDG Goal1: The Role of Payments Digitisation'. Available at: https://bhmng.com/achieving-sdg-goal-1-role-payments-digitisation-mike-ogbalu/

Ogbuji, C. N., Onuoha, C. B. and Izogo, E. E. (2012). 'Analysis of the Negative Effects of the Automated Teller Machine (ATM) as a Channel for Delivering Banking Services in Nigeria*',* *International Journal of Business and Management,* **7**(7), p. 180.

Ojo, A. (2017). 'The Role of Internal Auditors in Fraud Prevention', unpublished MBA thesis: Faculty of Business Economics and Tourism, University of Applied Science, Finland.

Okaro, S., Okafor, G. Nwanna, I. and Igbinovia, I. (2017). ‘Empowering the Internal Audit Function for Effective Role in Risk Management: A Study of Micro Finance Banks in Anambra State, South East, Nigeria’, *International Journal of Academic Research in Accounting, Finance and Management Sciences,* **7**(3), pp. 14-23.

Okoli, C. and Schabram, K. (2010). ‘A Guide to Conducting a Systematic Literature Review Of Information Systems Research’, *Sprouts: Working Papers on Information Systems,* **10**(26).

Okoye, A. (2017). ‘Organisational Fraud and the Role of Whistle-Blowers in Nigeria: A Critical Appraisal’, *Qmlj,* **8**, p. 35.

Olatunji, O. C. and Adekola, D. R. (2017). ‘The Roles of Auditors in Fraud Detection and Prevention in Nigeria Deposit Money Banks Evidence from Southwest’, *European Scientific Journal,* **13**(31).

Omodunbi, B., Odiase, P. Olaniyan, O. and Esan, A. (2016). ‘Cybercrimes in Nigeria: Analysis, Detection and Prevention’, *Journal of Engineering and Technology,* **1**(1).

Omogbhemhe, M. I. and Bayo, M. I. (2017). ‘A Multi-Factor Biometric Model for Securing E-banking System’, *International Journal of Computer Applications,* **159**(4).

Oni, A. A. and Ayo, C. K. (2010). ‘An Empirical Investigation of the Level of Users’ Acceptance of E-banking in Nigeria’, *Journal of Internet Banking and Commerce,* **15**(1), pp. 1-13

Onomza, W. V., Alhassan, J. Ismaila, I. and Tunde, A. (2015). ‘Plastic Financial Fraud in the Most Populated Black Africa; Nigeria: The Mitigation Based-on One-Time Password’, *Ijitr,* **3**(2), pp. 1868-1881.

Onyesolu, M. O. and Okpala, A. C. (2017). ‘Improving Security Using a Three-tier Authentication for Automated Teller Machine (ATM)’, *International Journal of Computer Network and Information Security,* **9**(10), p. 50.

Orlikowski, W. J. and Baroudi, J. J. (1991). ‘Studying Information Technology in Organizations: Research Approaches and Assumptions’, *Information Systems Research,* **2**(1), pp. 1-28.

Osei-Kyei, R., Chan, A. P. and Ameyaw, E. E. (2017). ‘A Fuzzy Synthetic Evaluation Analysis of Operational Management Critical Success Factors for Public-Private Partnership Infrastructure Projects’, *Benchmarking: An International Journal,* **24**(7), pp. 2092-2112.

Oye, N.D. and Nathaniel, J., (2018). 'Fraud Detection and Control System in Bank Using Finger Print Simulation', *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, **3**(1), pp. 1557-1567.

Pallant, J. (2013). *SPSS Survival Manual*. Berkshire, McGraw-Hill Education.

Pam, V. and Ozoya, M. (2016). 'Fraud Victims' Reaction and Crime Prevention in Nigeria: The Role of a Knowledge Economy', *Covenant University Journal of Politics and International Affairs,* **4**(1).

Pandy, S. (2017). 'Understanding the U.S. Card-not-Present (CNP)1 Fraud Landscape and Identifying Key CNP Fraud Mitigation Tools and Strategies'. Available at: https://www.bostonfed.org/-/media/Documents/PaymentStrategies/mpiw-cnp-fraud-brief.pdf.

Parisa, A. (2006). 'Adoption of E-banking Services by Iranian Customers, unpublished MSc thesis', Lulea University of Technology, Sweden.

Pierson, G. and DeHaan, J. (2015). 'Network Security and Fraud Detection System and Method*', U.S. Patent* **9**,*203,837.*

Pikkarainen, T., Pikkarainen, K. Karjaluoto, H. and Pahnila, S. (2004). 'Consumer Acceptance of Online Banking: An Extension of the Technology Acceptance Model', *Internet Research,* **14**(3), pp. 224-235.

Pinto, J. K. and Slevin, D. P. (1988). 'Critical Success Factors Across the Project Life Cycle'. *International Journal of Managing Projects in Business,* **5**(4), pp. 757-775,

Podsakoff, P. M., MacKenzie, S. B., Lee, J. Y., and Podsakoff, N. P. (2003). 'Common Method Biases in Behavioral Research: A Critical Review of the Literature and Recommended Remedies', *Journal of Applied Psychology,* **88** (5), pp. 879–903.

Poong, Y., Eze, U. C. and Talha, M. (2009). 'B2C E-commerce in Malaysia: Perceived Characteristics of Innovating and Trust Perspective', *International Journal of Electronic Business,* **7**(4), pp. 392-427.

Popo-ola, A. and Olowookere, S. (2008). 'Accessing E-banking Based on Resilient Transaction', unpublished MBA thesis: Department of Computer Science, Blekinge Institute of Technology, Sweden.

Povey, I. C. (2008). ‘Assessing the Impact of EMV Migration: A Pragmatic Delivery Approach’, *Journal of Payments Strategy & Systems*, **2**(4), pp. 349-363.

Prakash, A. and Malik, G. (2008). ‘Empirical Study of Internet Banking in India’, *CURIE Journal,* **1**(3).

Prenzler, T. (2016). ‘Welfare Fraud Prevention in Australia: A Follow-Up Study’, *Crime Prevention & Community Safety,* **18**(3), pp. 187-203.

PRWEB. (2010). ‘AuthenWare Expands Financial Services Clientele by Nearly a Half-Million Portals’. Available at: http://www.prweb.com/releases/2010/02/prweb3525574.htm

Puhakainen, P. and Siponen, M. (2010). ‘Improving Employees Compliance Through Information Systems Security Training: An Action Research Study*’, Mis Quarterly,* pp. 757-778.

Pulz, J., Muller, R. B. Romero, F. Meffe, A. Garcez Neto, A. F. and Jesus, A. S. (2017). *Fraud Detection in Low-Voltage Electricity Consumers Using Socio-economic Indicators and Billing Profile in Smart Grid*s. Institution of Engineering and Technology, **1**.

Patton, M. Q (2002). *Qualitative Research and Evaluation Methods*. California. Sage Publishers.

Rahman, R. A. and Anwar, I. S. K. (2014). ‘Effectiveness of Fraud Prevention and Detection Techniques in Malaysian Islamic Banks*’, Procedia-Social and Behavioral Sciences,* ***14*****5**, pp. 97-102.

Raja, V. (2012). ‘Global E-banking Scenario and Challenges in Banking System’, *Asian Journal of Research in Banking and Finance,* **2**(3), pp. 92-101.

Raju, K. K. and Murthi, R. (2011). ‘Fraud Risk Management’, *Journal of Business Management and Economics,* **9,** p. 4.

Ramakrishnan, G. (2001). ‘Risk Management for Internet Banking’, *Information Systems Control Journal*, **6**, pp. 48-51.

Randolph, J. J. (2009). ‘A Guide to Writing the Dissertation Literature Review’, *Practical Assessment, Research & Evaluation,* **14**(13), pp. 1-13.

Ratiu, C., Craciun, M. and Bucerzan, D. (2011). ‘Statistical Model of the People Confidence in E-business Services’, *Analele Universitatii Maritime Constanta,* **11**(14).

Reavley, N. (2005). ‘Securing Online Banking’, *Card Technology Today,* **17**(10), pp. 12-13.

Reed, M. (2005) ‘Reflections on the ‘Realist Turn’ in Organization and Management Studies’, *Journal of Management Studies,* **42**, pp. 1621–44.

Remenyi, D. and Williams, B. (1996). ‘The Nature of Research: Qualitative or Quantitative, Narrative or Paradigmatic?’, *Information Systems Journal,* **6**(2), pp. 131-146.

Remenyi, D. and Williams, B. (1998). *Doing Research in Business and Management: An introduction to Process and Method.* Sage Publications.

Revett, K., De Magalhães, S. T. and Santos, H. (2005). ‘Data Mining a Keystroke Dynamics Based Biometrics Database Using Rough Sets’, *Artificial Intelligence,* p. 188-191.

Rhee, H., Kim, C. and Ryu, Y. U. (2009). ‘Self-efficacy in Information Security: Its Influence on End Users' Information Security Practice Behavior’, *Computers & Security,* **28**(8), pp. 816-826.

Riedl, R., Roithmayr, F. Schenkenfelder, B. and Sprague, R. H. J. (2007). ‘Using the Structured-Case Approach to Build Theory in E-government’, *In System Sciences, 2007,* pp. 93-93.

Rizzardi, R. (2008). ‘Financial Management -- Payment Card Fraud can Happen to You’, *Optometry & Vision Development,* **39**(2), pp. 64-65.

Roberds, W. (1998). ‘The Impact of Fraud on New Methods of Retail Payment*’, Economic Review-Federal Reserve Bank of Atlanta,* **83**(1), p. 42.

Roberts, C. (2007). ‘Biometric Attack Vectors and Defences’, *Computers & Security,* **26**(1), pp. 14-25.

Roberts, L. D. and Allen, P. J. (2015). ‘Exploring Ethical Issues Associated with Using Online Surveys in Educational Research’, *Educational Research and Evaluation,* **21**(2), pp. 95-108.

Robinson, C. (2002). *Real World Research: A Resource for Social Scientists and Practitioner-Researchers*. Blackwell Pushers.

Rocco, T. S., Bliss, L. A. Gallagher, S. and Pérez-Prado, A. (2003). 'Taking the Next Step: Mixed Methods Research in Organizational Systems', *Information Technology, Learning, and Performance Journal,* **21**(1), p. 19.

Rockart, J. F. (1979). 'Chief Executives Define their Own Data Needs', *Harvard Business Review,* **57**(2), pp. 81-93.

Rorty, R. (1993). 'Consciousness, Intentionality, and Pragmatism', *Folk Psychology and the Philosophy of Mind*, pp. 388-404.

S. Sproule, and N. Archer. (2007). *Defining Identity Theft.* Management of eBusiness, Eighth World Congress, Toronto, IEEE

Safa, N. S. and Von Solms, R. (2016). 'An Information Security Knowledge Sharing Model in Organizations*', Computers in Human Behaviour,* **57**, pp. 442-451.

Salameh, R., Al-Weshah, G. Al-Nsour, M. and Al-Hiyari, A. (2011). 'Alternative Internal Audit Structures and Perceived Effectiveness of Internal Audit in Fraud Prevention', *Canadian Social Science,* **7**(3), p. 40.

Salimon, M. G., Yusoff, R. Z. and Mohd Mokhtar, S. S. (2016). 'What Determines Adoption of E-banking Among Nigerians? A Conceptual Approach', *Journal of Emerging Economies & Islamic Research,* **4**(2), pp. 1-12.

Salimon, M. G.,Yusoff, R. Z. and Moktar, S. M. (2017). 'The Mediating Role of Hedonic Motivation on the Relationship between Adoption of E-banking and its Determinants', *International Journal of Bank Marketing,* **35**(4), pp. 558-582.

Sari, R. P. (2015). 'Integration of Key Performance Indicator into the Corporate Strategic Planning: Case study at PT. Inti Luhur Fuja Abadi, Pasuruan, East Java, Indonesia*', Agriculture and Agricultural Science Procedia,* **3**, pp. 121-126.

Sasse, M. A. and Flechais, I. (2005). *Usable Security: Why do We Need It? How Do We Get It?.* Sebastopol, O'Reilly.

Sathye, M. (1999). 'Adoption of Internet Banking by Australian Consumers: An Empirical Investigation', *International Journal of Bank Marketing,* **17**(7), pp. 324-334.

Saunders, M., Lewis, P. and Thornhill, A. (2009). 'Understanding Research Philosophies and Approaches', *Research Methods for Business Students,* **4**, pp.122-143.

Saunders, M. (2011). *Research Methods for Business Students, 5/e.* Pearson Education India.

Saunders, M., Lewis, P. and Thornhill, A. (2012). *Research Methods for Business Students: 6th edition*. UK, Essex, Pearson Education Limited.

Saunders, S. (2003). 'Structural Realism, Again', *Synthese,* **136**(1), pp. 127-133.

Seang, G. S. (2003). Best Practices in KPI. *National Conference of Key Performance Indicators,* pp. 21-23.

Sebora, T. C., Lee, S. M. and Sukasame, N. (2009). 'Critical Success Factors for E-commerce Entrepreneurship: An Empirical Study of Thailand', *Small Business Economics,* **32**(3), pp. 303-316.

Seegar, M. (2005). *Apparatus and Method for Preventing Credit Card Fraud.* U.S. Patent 6,955,294.

Selim, H. M. (2007). 'Critical Success Factors for E-learning Acceptance: Confirmatory Factor Models*', Computers & Education,* **49**(2), pp. 396-413.

Seltzer, L. (2008). 'Measuring Identity Theft at Top Banks*', PC Magazine,* **27**(7), pp. 104-104.

Scandura, T. A. and Williams, E. A. (2000). 'Research Methodology in Management: Current Practices, Trends, and Implications for Future Research', *Academy of Management Journal,* **43**(6), pp. 1248-1264.

Scheuren, F. (2004). '*What is a Survey?* American Statistical Association'. Available at: *https://psr.iq.harvard.edu/american_statistical_association_what_a_survey*

Schreft, S. L. (2007). 'Risks of Identity Theft: Can the Market Protect the Payment System?', *Economic Review-Federal Reserve Bank of Kansas City,* **92**(4), p. 5.

Shah, M. H. and Siddiqui, F. A. (2006). 'Organisational Critical Success Factors in Adoption of E-banking at the Woolwich Bank*', International Journal of Information Management,* **26**(6), pp. 442-456.

Shah, M. (2009). *E-banking management: Issues, Solutions, and Strategies: Issues, Solutions, and Strategies*. London IGI Global.

Shah, M. H., Braganza, A. and Morabito, V. (2007). ‘A Survey of Critical Success Factors in E-banking: An Organisational Perspective*’, European Journal of Information Systems,* **16**(4), pp. 511-524.

Shah, M. H., Ahmed, J. and Soomro, Z. A. (2016). ‘Investigating the Identity Theft Prevention Strategies in M-commerce’. International Conferences ITS, Melbourne, December.

Shaji, N. A. and Soman, S. (2017). ‘Multi-factor Authentication for Net Banking’, *International Journal of System & Software Engineering,* **5**(1), pp. 11-14.

Shank, M. E., Boynton, A. C. and Zmud, R. W. (1985). ‘Critical Success Factor Analysis as a Methodology for MIS Planning*’, MIS Quarterly,* pp. 121-129.

Shanmugapriya, D. and Padmavathi, G. (2009). ‘A Survey of Biometric Keystroke Dynamics: Approaches, Security and Challenges’, *ArXiv*.

Sheatsley, P. B. (1983). ‘Questionnaire Construction and Item Writing’, *Handbook of Survey Research,* **4**(1), pp. 195-230.

Shen, Q. (2009). ‘Case Study in Contemporary Educational Research: Conceptualization and Critique/Etudes de cas dans la Recherche Pedagogique Contemporaine: Conceptualisation et Critique’, *Cross-Cultural Communication,* **5**(4), p. 21.

Shlens, J. (2014). *A Tutorial on Principal Component Analysis.* Google Research, Mountain View.

Sidden, K. and Simmons, D. (2005). ‘Banking on Security*’, American City & County,* **120**, pp. 11-30.

Siddiqui, A.A. and Qureshi, R. (2017). ‘Big Data In Banking: Opportunities And Challenges Post Demonetisation in India’, *Journal of Computer Engineering,* pp. 33-39.

Simon, A. (2015). ‘Program Key Performance Indicators (KPIs) and Key Operating Indicators (KOIs)’, Waltham, Elsevier, pp. 65-72.

Singh, N. (2007). ‘Online Frauds in Banks with Phishing’, *Journal of Internet Banking & Commerce,* **12**(2).

Skibniewski, M. J. and Ghosh, S. (2009). ‘Determination of Key Performance Indicators with Enterprise Resource Planning Systems in Engineering Construction Firms*’, Journal of Construction Engineering & Management,* **135**(10), pp. 965-978.

Smith, M. J. (1998). *Social Science in Question: Towards a Post Disciplinary Framework*. Sage Publications.

Somers, T. M. and Nelson, K. (2001). ‘The Impact of Critical Success Factors Across the Stages of Enterprise Resource Planning Implementations’, *System Sciences,* p. 10.

Songini, M. L. (2004). ‘Fraud Sniffers*’, Computerworld,* **38**(25), pp. 42-42.

Sood, A. and Enbody, R. (2011). ‘The State of HTTP Declarative Security in Online Banking Websites’, *Computer Fraud & Security,* **2011**(7), pp. 11-16.

Sravanthi, G. (2016). ‘Management of Risk Issues in E-banking - A Case Study’, *International Journal of Recent Research Aspects,* **3**(3), pp. 38-44.

Stevens, J. (1996). ‘Exploratory and Confirmatory Factor Analysis’, *Applied Multivariate Statistics for the Social Sciences,* pp. 362-428.

Stone, D. (1978). ‘The Human Potential Movement’, *Society,* **15**(4), pp. 66-68.

Streff, K. (2009). ‘An Information Security Management System Model for Small and Medium-Sized Financial Institutions*’, Issues in Information Systems,* **10**(2). pp. 650 - 659

Suhr, D.D. (2005). ‘Principal Component Analysis vs. Exploratory Factor Analysis’. In the Proceedings of the 30th Annual SAS Users Group International Conference, Cary, NC, April.

Sun, Q., Simon, D. R. Wang, Y. Russell, W. Padmanabhan, V. N. and Qiu, L. (2002). ‘Statistical Identification of Encrypted Web Browsing Traffic’, IEEE Symposium on Security and Privacy, California, May.

Swafford, P. M., Ghosh, S. and Murthy, N. (2006). 'The Antecedents of Supply Chain Agility of a Firm: Scale Development and Model Testing', *Journal of Operations Management,* **24**(2), pp. 170-188.

Swanson, R. A. and Holton, E. F. (2005). *Research in Organizations: Foundations and Methods in Inquiry.* San Francisco, Berrett-Koehler Publishers.

Tabachnick, B. G. and Fidel, L. S. (2001). *Using Multivariate Statistics*. Essex, UK, Pearson Education Limited

Tade, O. and Adeniyi, O. (2017). 'Automated Teller Machine Fraud in South-West Nigeria: Victim Typologies, Victimisation Strategies and Fraud Prevention', *Journal of Payments Strategy & Systems,* **11**(1), pp. 86-92.

Taiwo, J., Agwu, M., Babajide, A. Okafor, T. C. and Isibor, A. A. (2016). 'Growth of Bank Frauds and the Impact on the Nigerian Banking Industry', *Journal of Business Management and Economics,* **4**(12), pp. 1-10.

Tam, L., Glassman, M. and Vandenwauver, M. (2010). 'The Psychology of Password Management: A Tradeoff Between Security and Convenience*', Behaviour & Information Technology,* **29**(3), pp. 233-244.

Tan, J. J., Titkov, L. and Poslad, S. (2002). 'Securing Agent-Based E-banking Services', *Workshop on Deception, Fraud and Trust in Agent Societies,* pp. 148-162.

Tarafdar, M. and Vaidya, S. D. (2006). 'Challenges in the Adoption of E-commerce Technologies in India: The Role of Organizational Factors', *International Journal of Information Management,* **26**(6), pp. 428-441.

Tatiana, A. (2017). 'Fraud Prevention by Government Auditors'. CISTI (Iberian Conference on Information Systems & Technologies / Conferência Ibérica De Sistemas e Tecnologias De Informação) Proceedings, **1**, pp. 307-312.

Teo, T. S. and Ang, J. S. (1999). 'Critical Success Factors in the Alignment of IS Plans with Business Plans', *International Journal of Information Management,* **19**(2), pp. 173-185.

Tinsley, H.E. and Tinsley, D.J. (1987). 'Uses of Factor Analysis in Counseling Psychology Research', *Journal of Counseling Psychology,* **34**(4), p. 414.

Titrade, C., Ciolacu, B. and Pavel, F. (2008). 'E-banking: Impact, *Risks, Security'*, *Annals of the University of Oradea, Economic Science Series*. **17**(4), pp. 1537-1542.

Torres, J. M., Sarriegi, J. M., Santos, J. and Serrano, N. (2006). 'Managing Information Systems Security: Critical Success Factors and Indicators to Measure Effectiveness'. International Conference on Information security, Samon, August.

Trim, P. R. J. and Yang-Im Lee. (2010). 'A Security Framework for Protecting Business, Government and Society from Cyber Attacks', *System of Systems Engineering (SoSE)*, pp. 1-6.

Trochim, W. M. and Donnelly, J. P. (2001). 'Research Methods Knowledge Base'. Available at: http://www.anatomyfacts.com/research/researchmethodsknowledgebase.pdf

Tsai, C., Chen, C. and Zhuang, D. (2012). 'Trusted M-banking Verification Scheme Based on a Combination of OTP and Biometrics', *Journal of Convergence,* **3**(3), pp. 23-30.

Tsai, W., Huang, B. Liu, J. Tsaur, T. and Lin, S. (2010). 'The Application of Web ATMs in E-payment Industry: A Case Study', *Expert Systems with Applications,* **37**(1), pp. 587-597.

TSE, W. K. D., HUI, M. H. LAM, S. T. MOK, Y. C. OEI, W. C. TANG, K. L. and YAU, X. L. (2013). 'Education in IT Security: A Case Study in Banking Industry', *GSTF Journal on Computing,* **3**(3), pp. 21-30.

Tu, Z. and Yuan, Y. (2014). 'Critical Success Factors Analysis on Effective Information Security Management: A Literature Review'. Twentieth Americas Conference on Information Systems, Savannah.

Tuchila, R. (2000). 'Servicii Bancare Prin Internet', *E-Finance Romania,* **3**(3), p. 23.

Ullman, J. B. and Newcomb, M. D. (1998). 'Eager, Reluctant, and Nonresponders to a Mailed Longitudinal Survey: Attitudinal and Substance Use Characteristics Differentiate Respondents', *Journal of Applied Social Psychology*, **28**, pp. 357-375.

Van Veen-Dirks, P. and Wijn, M. (2002). 'Strategic Control: Meshing Critical Success Factors with the Balanced Scorecard', *Long Range Planning,* **35**(4), pp. 407-427.

Vandommele, T. (2010). 'Biometric Authentication Today', Proceedings of the Seminar on Network Security. Available at: http://www.cse.hut.fi/en/publications/B/11/papers/vandommele.pdf

Veloso, A.A., Meira Jr, W. Parthasarathy, S. and De Carvalho, M.B. (2003). 'Efficient, Accurate and Privacy-Preserving Data Mining for Frequent Item Sets in Distributed Databases', *Computer Science*, **1**, p.1.

Verizon Enterprise (2014). 'Verizon 2014 Data Breach Investigations Report'. Available at: http://www.verizonenterprise.com/resources/reports/rp_Verizon-DBIR-2014_en_xg.pdf.

Verizon Enterprise. (2015). 'Global Fraud Report, 2015'. Available at: *Http://www.Krolladvisory.com/insights-reports/global-Fraud-Reports*

Verizon Enterprise. (2016). 'Data Breach Investigations Report'. Available at: http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf.

Verizon Enterprise. (2017). 'Data Breach Investigations Report'. Available at: http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/.

Virgo, G. (2007). 'Assisting the Victims of Fraud: The Significance of Dishonesty and Bad Faith', *Cambridge Law Journal,* **66**(1), pp. 22-24.

Voss, C., Tsikriktsis, N. and Frohlich, M. (2002). 'Case Research in Operations Management', *International Journal of Operations & Production Management,* **22**(2), pp. 195-219.

Vu, K. L., Proctor, R. W. Bhargav-Spantzel, A. Tai, B. Cook, J. and Eugene Schultz, E. (2007). 'Improving Password Security and Memorability to Protect Personal and Organizational Information', *International Journal of Human-Computer Studies,* **65**(8), pp. 744-757.

Wacker, J. G. (1998). 'A Definition of Theory: Research Guidelines for Different Theory-building Research Methods in Operations Management', *Journal of Operations Management,* **16**(4), pp. 361-385.

Waly, N., Tassabehji, R. and Kamala, M. (2012). 'Improving Organisational Information Security Management: The Impact of Training and Awareness', *High Performance Computing and Communication,* pp. 1270-1275.

Ward, J. M. (1990). ‘A Portfolio Approach to Evaluating Information Systems Investments and Setting Priorities’, *Journal of Information Technology*, **5**(4), p. 222.

Wei, W., Li, J. Cao, L. Ou, Y. and Chen, J. (2013). ‘Effective Detection of Sophisticated Online Banking Fraud on Extremely Imbalanced Data’, *World Wide Web*, **16**(4), pp. 449-475.

White, H. and Nteli, F. (2004). ‘Internet Banking in the UK: Why Are There Not More Customers?’, *Journal of Financial Services Marketing*, **9**(1), pp. 49-56.

Wilks, D. S. (2006). ‘Statistical Methods in the Atmospheric Sciences Second Edition’, *International Geophysics Series*, **91**, pp. 627.

Williams, J. and Ramaprasad, A. (1996). ‘A Taxonomy of Critical Success Factors’, *European Journal of Information Systems*, **5**(4), pp. 250-260.

Williams, G. (2014). ‘Cyber security: Whose Responsibility Is It?’, *Hydrocarbon Processing*, **93**(10), pp. 67-68.

Workman, M. (2008). ‘Wisecrackers: A Theory-grounded Investigation of Phishing and Pretext Social Engineering Threats to Information Security’, *Journal of the American Society for Information Science and Technology*, **59**(4), pp. 662-674.

World Bank. (2017). ‘The World Bank in Nigeria: Data’. Available at: http://www.worldbank.org/en/country/nigeria/overview

Wright, K. B. (2005). ‘Researching Internet-based populations: Advantages and Disadvantages of Online Survey Research, Online Questionnaire Authoring Software Packages, and Web Survey Services’, *Journal of Computer-Mediated Communication*, **10**(3).

Yaghoubi, N. M., Siavashi, R. and Bahmaei, R. (2016). ‘A Survey of Critical Success Factors of Private Banks in Electronic Banking Services’, *Modern Applied Science*, **10**(7), p. 115.

Yasar, N., Yasar, F. M. and Topcu, Y. (2012). *Operational Advantages of Using Cyber Electronic Warfare (CEW) in the Battlefield*. Baltimore, MD, USA.

Yeoh, W., Koronios, A. and Gao, J. (2008). *Managing the Implementation of Business Intelligence Systems: A Critical Success Factors Framework*. Business Science Reference, New York.

Yibin, M. (2003). ‘E-banking: Status, trends, Challenges and Policy Issues’, *CBRC Seminar the Development and Supervision of E-Banking Shanghai.* 2003.

Yin, R. K. (1981). ‘The Case Study as a Serious Research Strategy’, *Science Communication,* **3**(1), pp. 97-114.

Yin, R. K. (1994). ‘Discovering the Future of the Case Study. Method in Evaluation Research’, *Evaluation Practice,* **15**(3), pp. 283-290.

Yin, R. K. (2003). *Case Study Research Design and Methods Third Edition.,* London, UK, Sage Publications.

Yin, R. K. (2013). *Case Study Research: Design and Methods.* London, UK, Sage Publications.

Yung-Cheng Shen., Chun-Yao Huang. Chia-Hsien Chu. and Chih-Ting Hsu. (2010). ‘A Benefit-cost Perspective of the Consumer Adoption of the Mobile Banking System’, *Behaviour & Information Technology,* **29**(5), pp. 497-511.

Zafar, H., Clark, J. G. Ko, M. and Au, Y. A. (2011). *Critical Success Factors for an Effective Security Risk Management Program: An Exploratory Case Study at a Fortune 500 firm.* Red Hook, Curran.

Zainal, Z. (2017). ‘Case Study as a Research Method’, *Jurnal Kemanusiaan,* **5**(1).

Zali, H., Farshadfar, E. and Sabaghpour, S. (2011). ‘Non-parametric Analysis of Phenotypic Stability in Chickpea Genotypes in Iran’. Crop Breeding Journal, **1**, pp. 89-100.

Zoldi, S. (2015). ‘Using Anti-Fraud Technology to Improve the Customer Experience’, *Computer Fraud & Security*, ***2015*** (7), pp. 18-20.

Zou, S., David, M., Andrus, D. and Norvell, W. (1997). ‘Standardization of international marketing strategy by firms from a developing country’, *International Marketing Review,* **14**(2), pp. 107-123.

APPENDIX A: Literature Review Process

A systematic literature review was carried out in the area of focus, e-banking fraud prevention. Several keywords were used for searching databases to find relevant literature for the review. They are given below:

- Electronic Banking Fraud
- Electronic Banking Fraud Prevention Technology/Security/Measures/Software
- Electronic Banking Security
- Fraud Prevention
- Fraud Prevention Factors
- Fraud Prevention Measures
- Fraud Prevention Critical Success Factors
- Online Banking Fraud

In addition, the above keywords were replicated with the additional word “Nigeria” added to identify literature specific to the Nigerian context. In order to perform searches for relevant literature, the following databases were selected for use:

- Academic Search Complete
- Business Source Complete
- Computers & applied sciences complete
- EBSCOhost EJS
- Emerald Management e-Journals
- Google Scholar
- Science Direct

Whilst searching, advanced search features such as applying related words and searching within the full text of articles were utilised. After each search had been completed, the results were reviewed, and the most relevant literature was selected for use. The internet search engine was used to identify websites and reports which also published relevant information related to the aforementioned areas. These were also reviewed, filtered and referenced during the literature review phase. All papers, articles and reports were then used to form a summary of related literature.

APPENDIX B: Questionnaire Instrument

A Survey on Critical Success Factors for E-Banking Fraud Prevention in Nigeria

E-Banking fraud is an issue being experienced globally and is continuing to prove costly to both banks and customers. Frauds in e-banking services occur as a result of various compromises in security ranging from weak authentication systems to insufficient internal controls. This survey will be used to help investigate factors that are critical to the prevention of fraud over electronic banking mediums in Nigeria. The main objectives of the questionnaire are:

- To determine the factors most critical to the success of preventing fraud over the e-banking medium
- To identify the security and fraud prevention measures organisations have introduced and the impact they have had

All information given will be treated in **strict confidence** and will only be used for research purposes.

PARTICIPANT DEMOGRAPHICS

Q 1. In order for us to classify your answers and make statistical analysis, please provide the following details.

Gender	
How many years of experience do you have working with e-banking security?	Below 1 [ ], 1 - 5 [ ], 6 - 10 [ ], 11 - 15 [ ], 16 - 20 [ ]
Email Address	

CLASSIFICATION OF E-BANKING FRAUD PREVENTION MEASURES

Q 2. Kindly rate the following strategic factors in terms of their criticality for e-banking fraud prevention. 1 indicates the lowest criticality whilst 5 indicates the highest criticality. Please only tick one box for each question.

		CRITICALITY **[Low]**		**[Moderate]**		**[High]**
No	**Factor**	**1**	**2**	**3**	**4**	**5**
Strategic Factors						
1	Timely access to information to empower decision making					
2	Mitigation of consumer vulnerability to fraud by providing adequate Consumer Education					
3	Awareness of Socio-Economic climate					
4	Engaging Consultants/Specialists					
5	Organisation learning for fraud prevention					
6	Adaptive Policies, Procedures and Controls					
7	Use of specialist third parties as intermediaries for online transactions to enhance confidentiality.					
8	Using historical data for intelligence to determine probability of fraud during each transaction					

Q 3. The following factors have been identified as operational factors that may prevent e-banking fraud. Kindly rate them in terms of their criticality for e-banking fraud prevention. 1 indicates the lowest criticality whilst 5 indicates the highest criticality. Please only tick one box for each question.

		CRITICALITY **[Low]**		**[Moderate]**		**[High]**
No	**Factor**	**1**	**2**	**3**	**4**	**5**
Operational Factors						
9	Top Management Support					
10	Financial Resources					
11	Management and Employees Readiness to Change					
12	Adequate Change Management					
13	Regular internal Audits					

14	Strict Customer Data Protection					
15	Security Specialist Team					
16	Strict Internal Controls					
17	Responsive customer service team					

Q 4. The following factors have been identified as technological factors that may prevent e-banking fraud. Kindly rate them in terms of their criticality for e-banking fraud prevention. 1 indicates the lowest criticality whilst 5 indicates the highest criticality. Please only tick one box for each question.

		CRITICALITY **[Low]**		**[Moderate]**		**[High]**
No	**Factor**	**1**	**2**	**3**	**4**	**5**
Technological Factors						
18	Using Biometrics to strengthen Authentication Systems					
19	Using data encryption					
20	Using One Time Passwords as an additional method of authentication					
21	Using Smart Cards for Authentication					
22	Using Strong Passwords (Passwords that consist of both letters and numbers and are a minimum of 8 characters)					
23	Using Multi-Layer Passwords					
24	Using artificial intelligence systems to work with fraud patterns and behaviours to predict, alert and prevent fraud					
25	Scalability of the Security Systems					
26	Ensuring User friendliness of system					
27	Availability of Authentication Solutions that are economically viable					
28	Integration of Solutions					

Q 5. From your experience, please highlight any other factors that may help prevent fraud through e-banking mediums.

…………………………………………………………………………………………

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

Q 6. Will you like to participate\ in a case study that will be conducted as part of this research? A brief interview will be required and will be arranged at your convenience.

Yes [ ] **No** [ ]

Q 7. Would you like to receive a summary of the findings from this research?

Yes [ ] **No** [ ]

Thank you for taking time out to complete this questionnaire. As earlier stated, information provided will be kept strictly confidential. Please do not hesitate to contact me with any queries using the contact details below:

Ahmad Kabir Usman
Researcher in E-banking Fraud Prevention
Lancashire Business School
University of Central Lancashire
Preston, UK

Ausman2@uclan.ac.uk

APPENDIX C: Questionnaire Pilot Feedback Form

The purpose of the pilot exercise is to ensure quality, relevance and ease of use of the survey. Your feedback is therefore essential. Kindly review the survey and answer the questions below.

	ANSWER	
QUESTIONS	**YES**	**NO**
1. Do you understand the objective of the survey?		
2. Is the wording of the survey clear?		
3. Are the answer choices suitable for the questions?		
4. Do any of the items require you to think too long or hard before responding? If so, which one(s)?		
5. Do any of the questions produce irritation, embarrassment, or confusion? If so, which one(s)?		
6. Do any of the questions generate response bias? If so, which one(s)?		
7. Is the survey too long?		
8. Does the survey make use of appropriate headings?		
9. Does the survey make use of appropriate sections?		
10. Provide any recommendations on how to further improve the survey: …………………………………………………………………………………………… …………………………………………………………………………………………… …………………………………………………………………………………………… …………………………………………………………………………………………… …………………………………………………………………………………………… …………………………………………………………………………………………… ……………………………………………………………………………………………		

Thank you for completing the feedback form. Kindly return this form to Ahmad Kabir Usman (Ausman2@uclan.ac.uk), Researcher in E-banking Fraud Prevention, Lancashire Business School, University of Central Lancashire, Preston, UK

APPENDIX D: Normality Test

Tests of Normality – Strategic Factors

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
S1	.207	110	.000	.844	110	.000
S2	.232	110	.000	.846	110	.000
S3	.210	110	.000	.906	110	.000
S4	.229	110	.000	.890	110	.000
S5	.261	110	.000	.803	110	.000
S6	.228	110	.000	.832	110	.000
S7	.227	110	.000	.904	110	.000
S8	.280	110	.000	.770	110	.000

a. Lilliefors Significance Correction

Tests of Normality – Operational Factors

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
O9	.299	110	.000	.782	110	.000
O10	.306	110	.000	.767	110	.000
O11	.240	110	.000	.894	110	.000
O12	.174	110	.000	.913	110	.000
O13	.242	110	.000	.886	110	.000
O14	.302	110	.000	.785	110	.000
O15	.219	110	.000	.887	110	.000
O16	.257	110	.000	.890	110	.000
O17	.217	110	.000	.907	110	.000

a. Lilliefors Significance Correction

Tests of Normality – Technological Factors

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
T18	.257	110	.000	.809	110	.000
T19	.223	110	.000	.852	110	.000
T20	.253	110	.000	.824	110	.000
T21	.287	110	.000	.844	110	.000
T22	.201	110	.000	.891	110	.000
T23	.239	110	.000	.890	110	.000
T24	.298	110	.000	.808	110	.000

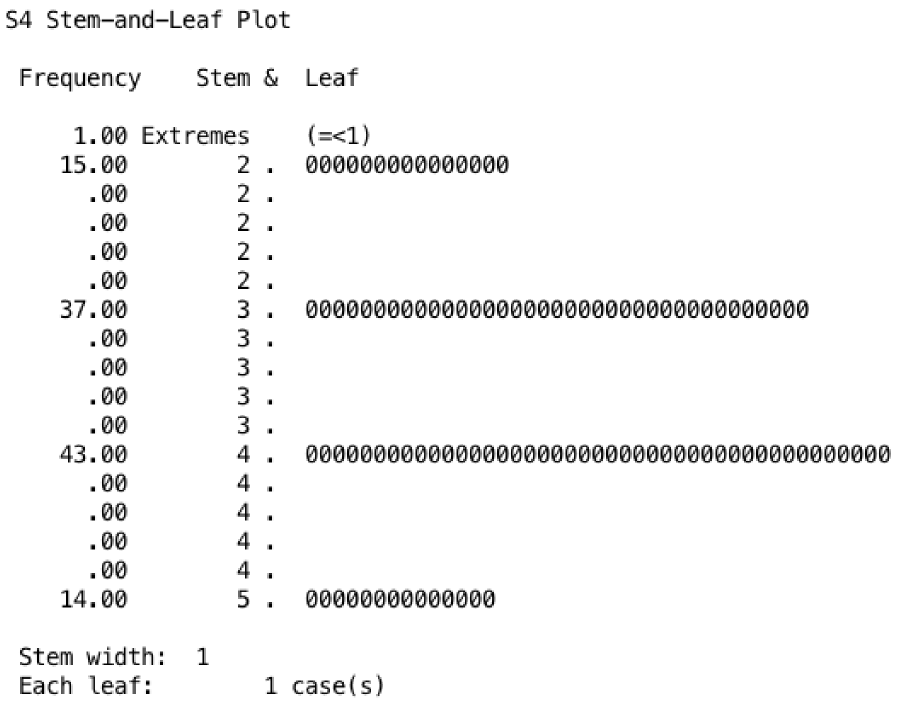
T25	.186	110	.000	.908	110	.000
T26	.199	110	.000	.871	110	.000
T27	.289	110	.000	.786	110	.000
T28	.187	110	.000	.908	110	.000
a. Lilliefors Significance Correction						

APPENDIX E: Outliers Analysis

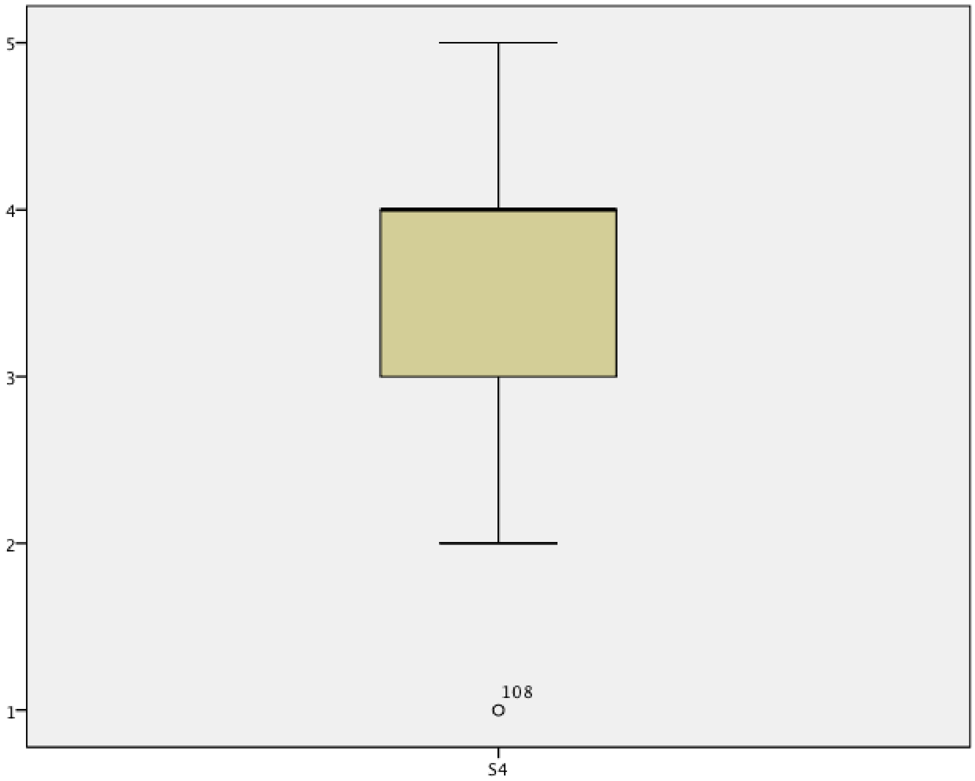
Strategic Factors

An outlier was identified in the results for one of the strategic factor variables. The diagram below presents the stem and leaf output and box plot highlighting the outlier from SPSS.

Variable S4



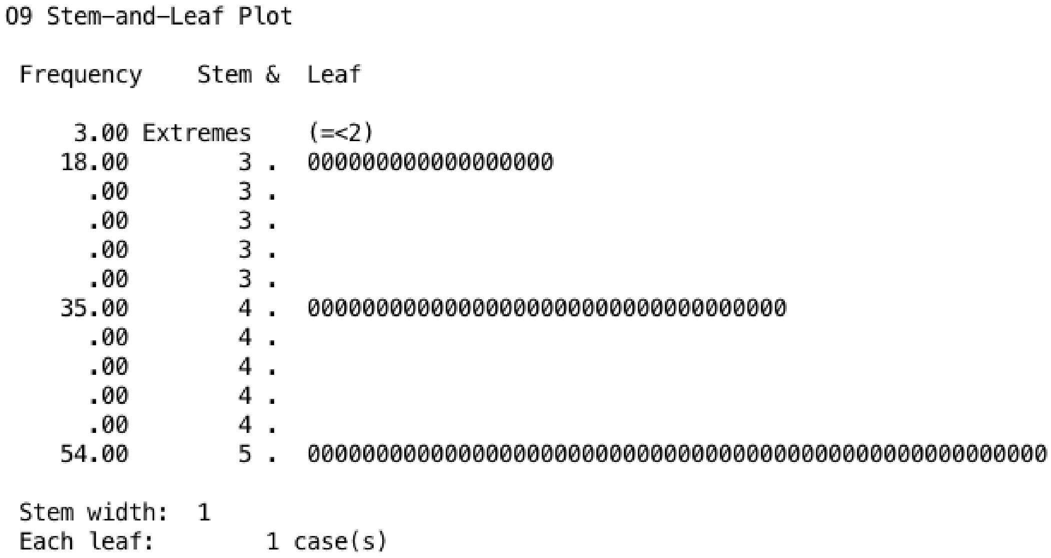
```
S4 Stem-and-Leaf Plot

 Frequency    Stem &  Leaf

     1.00 Extremes    (=<1)
    15.00        2 .  000000000000000
      .00        2 .
      .00        2 .
      .00        2 .
      .00        2 .
    37.00        3 .  0000000000000000000000000000000000000
      .00        3 .
      .00        3 .
      .00        3 .
      .00        3 .
    43.00        4 .  0000000000000000000000000000000000000000000
      .00        4 .
      .00        4 .
      .00        4 .
      .00        4 .
    14.00        5 .  00000000000000

 Stem width:   1
 Each leaf:        1 case(s)
```



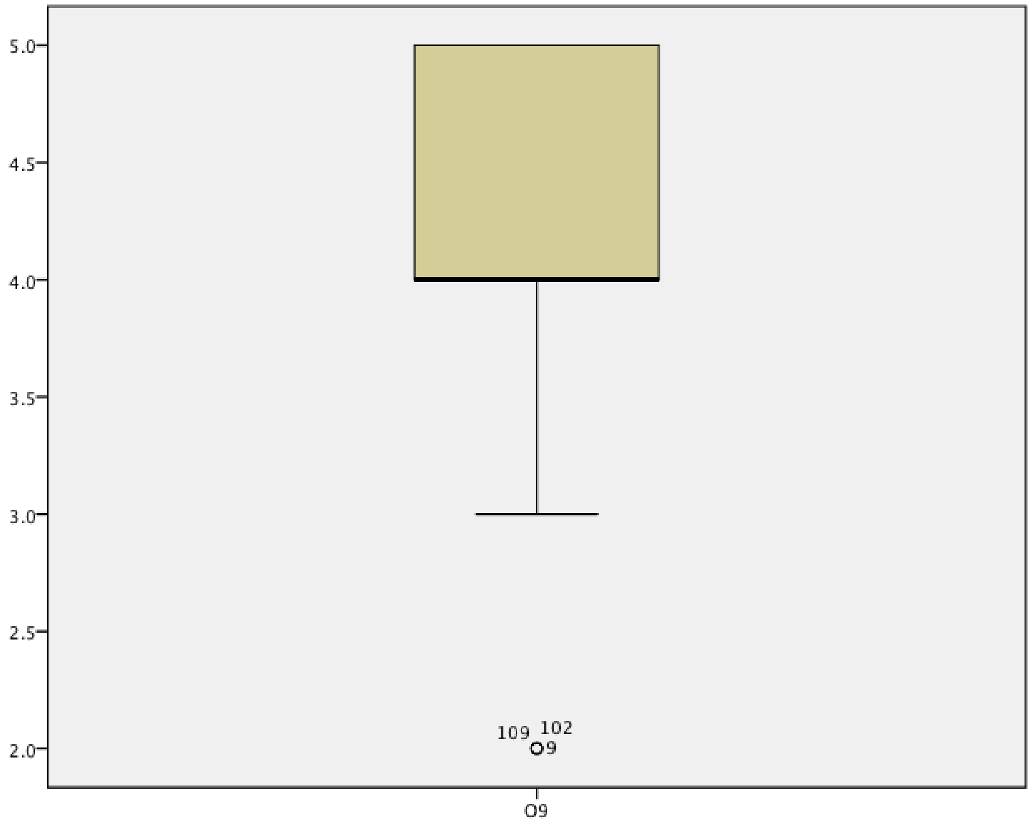
Operational Factors

Outliers were identified in the results for eight of the operational factor variables. The diagram below presents the stem and leaf output and box plot highlighting the outlier from SPSS.

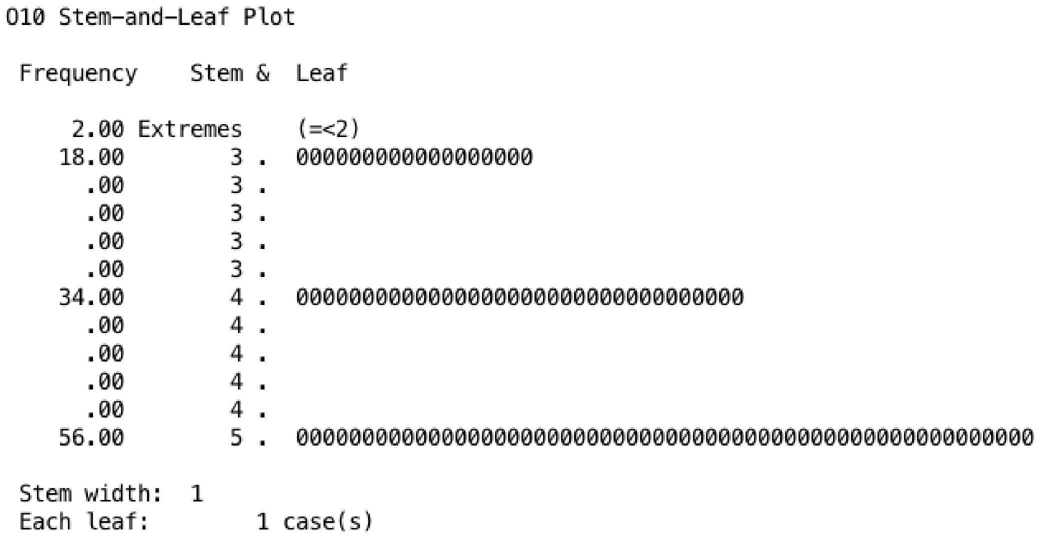
Variable O9



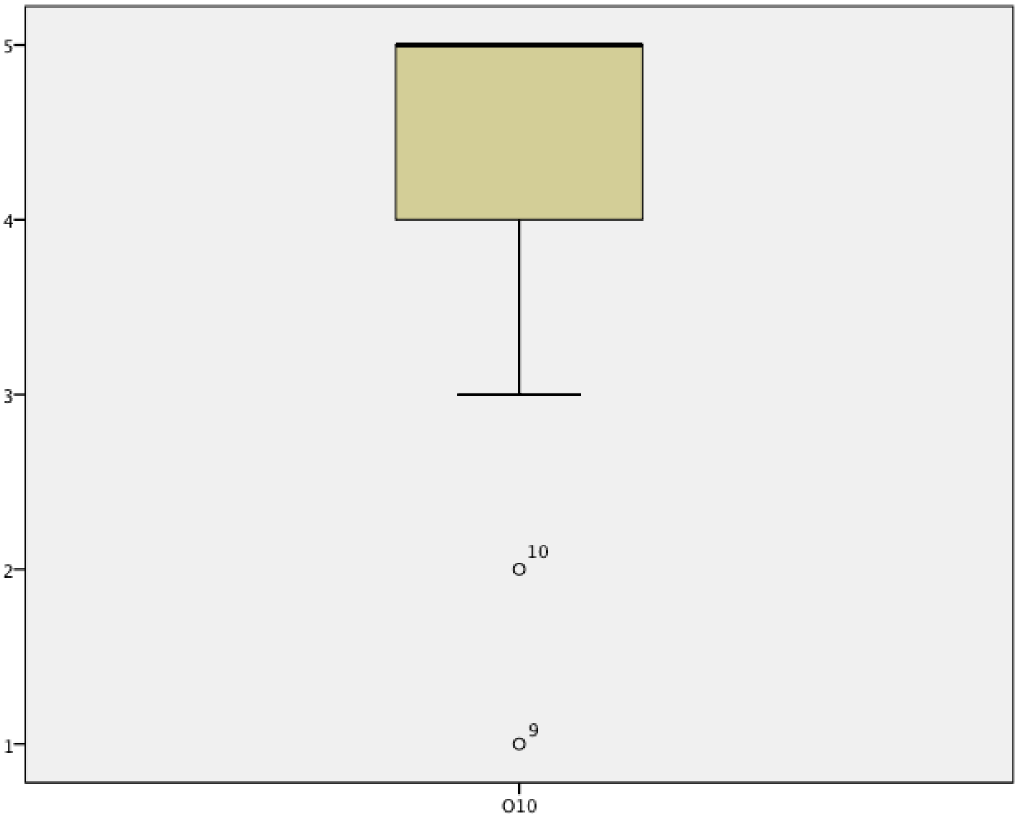
```
O9 Stem-and-Leaf Plot

 Frequency    Stem &  Leaf

     3.00 Extremes    (=<2)
    18.00        3 .  000000000000000000
      .00        3 .
      .00        3 .
      .00        3 .
      .00        3 .
    35.00        4 .  00000000000000000000000000000000000
      .00        4 .
      .00        4 .
      .00        4 .
      .00        4 .
    54.00        5 .  000000000000000000000000000000000000000000000000000000

 Stem width:   1
 Each leaf:        1 case(s)
```



Variable O10

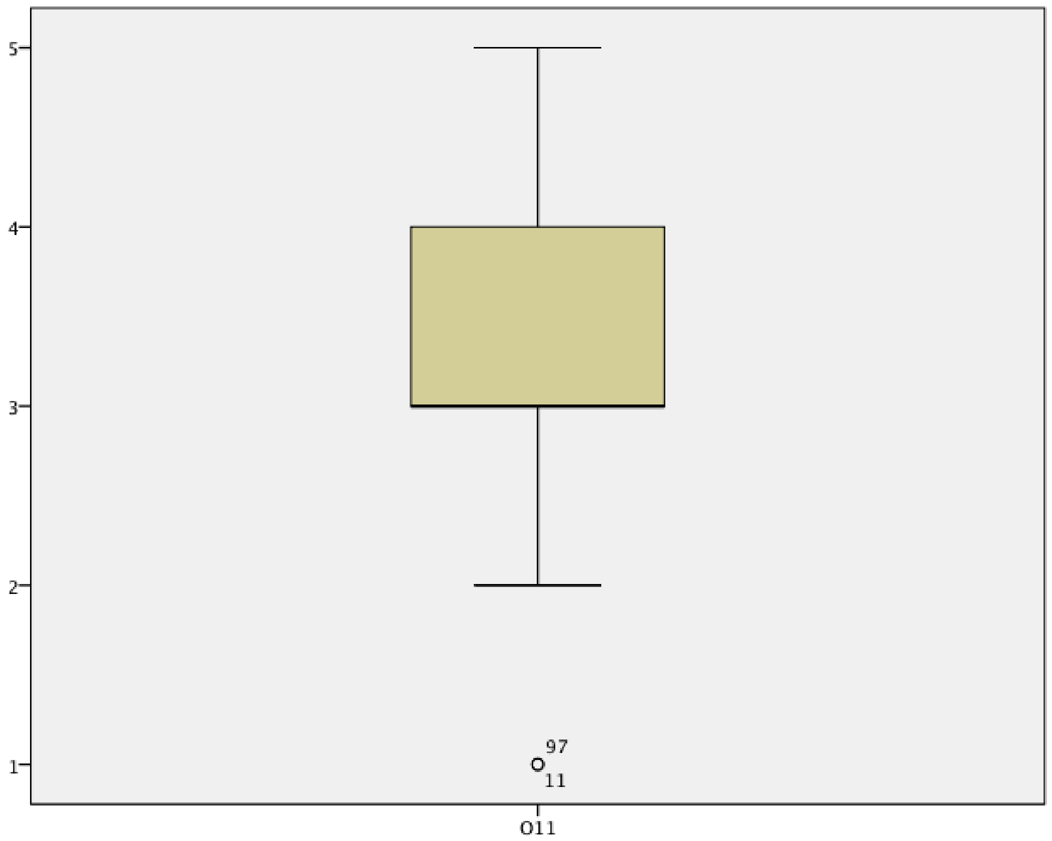


```
O10 Stem-and-Leaf Plot

 Frequency    Stem &  Leaf

     2.00 Extremes    (=<2)
    18.00        3 .  000000000000000000
      .00        3 .
      .00        3 .
      .00        3 .
      .00        3 .
    34.00        4 .  0000000000000000000000000000000000
      .00        4 .
      .00        4 .
      .00        4 .
      .00        4 .
    56.00        5 .  00000000000000000000000000000000000000000000000000000000

 Stem width:  1
 Each leaf:        1 case(s)
```

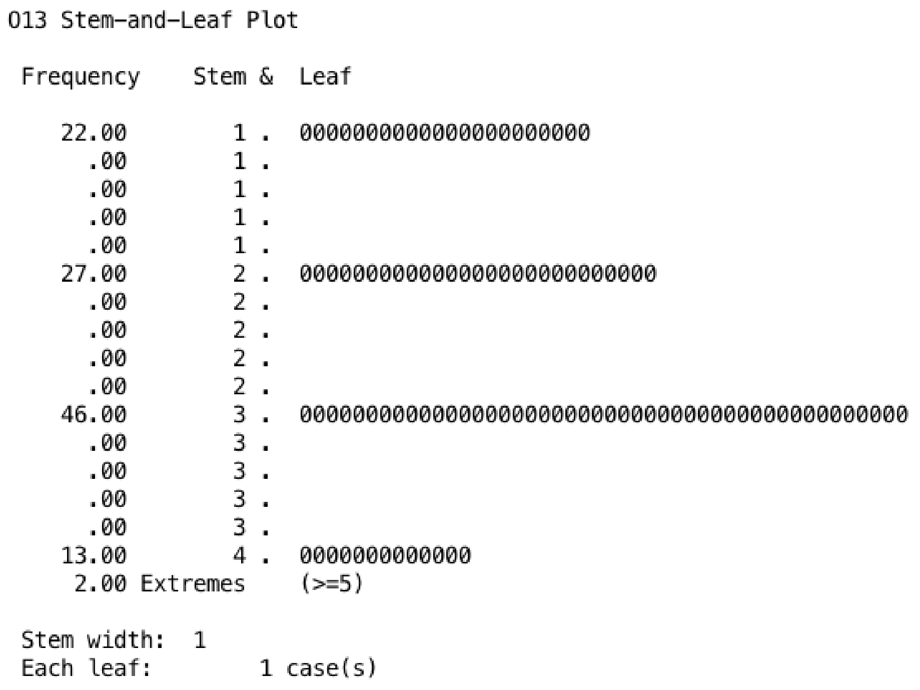


Variable O11

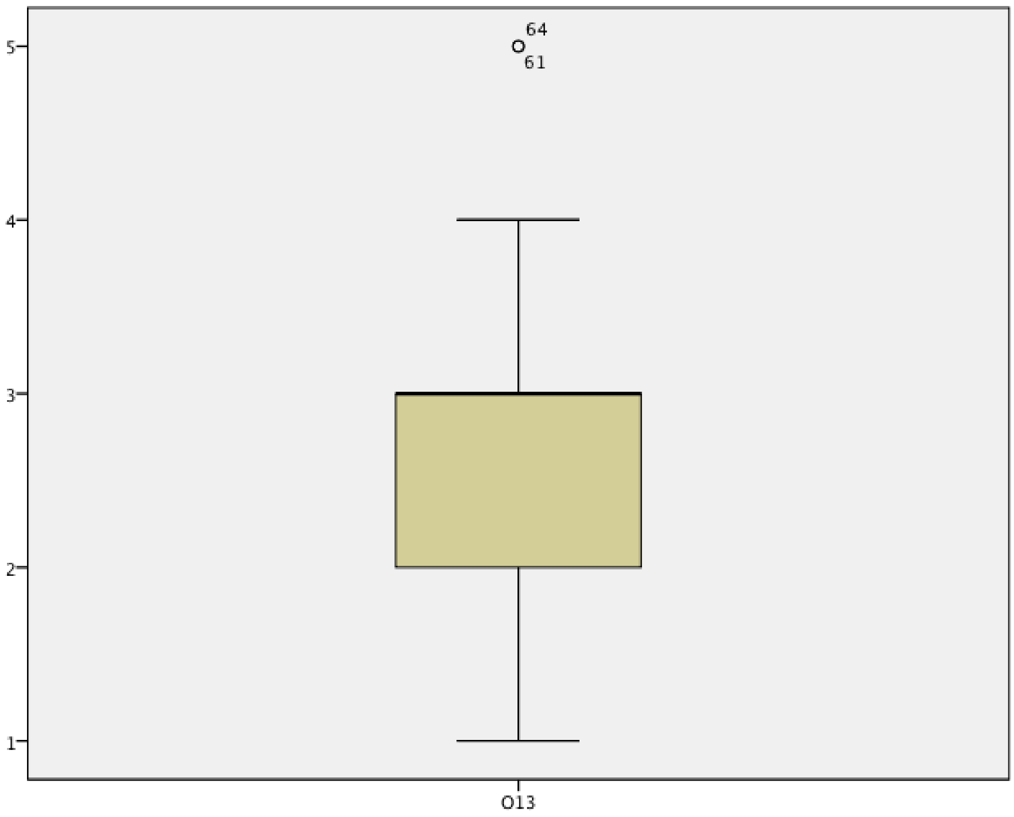
```
O11 Stem-and-Leaf Plot

 Frequency    Stem &  Leaf

     2.00 Extremes    (=<1)
    17.00        2 .  00000000000000000
      .00        2 .
      .00        2 .
      .00        2 .
      .00        2 .
    47.00        3 .  00000000000000000000000000000000000000000000000
      .00        3 .
      .00        3 .
      .00        3 .
      .00        3 .
    29.00        4 .  00000000000000000000000000000
      .00        4 .
      .00        4 .
      .00        4 .
      .00        4 .
    15.00        5 .  000000000000000

 Stem width:   1
 Each leaf:        1 case(s)
```



Variable O13

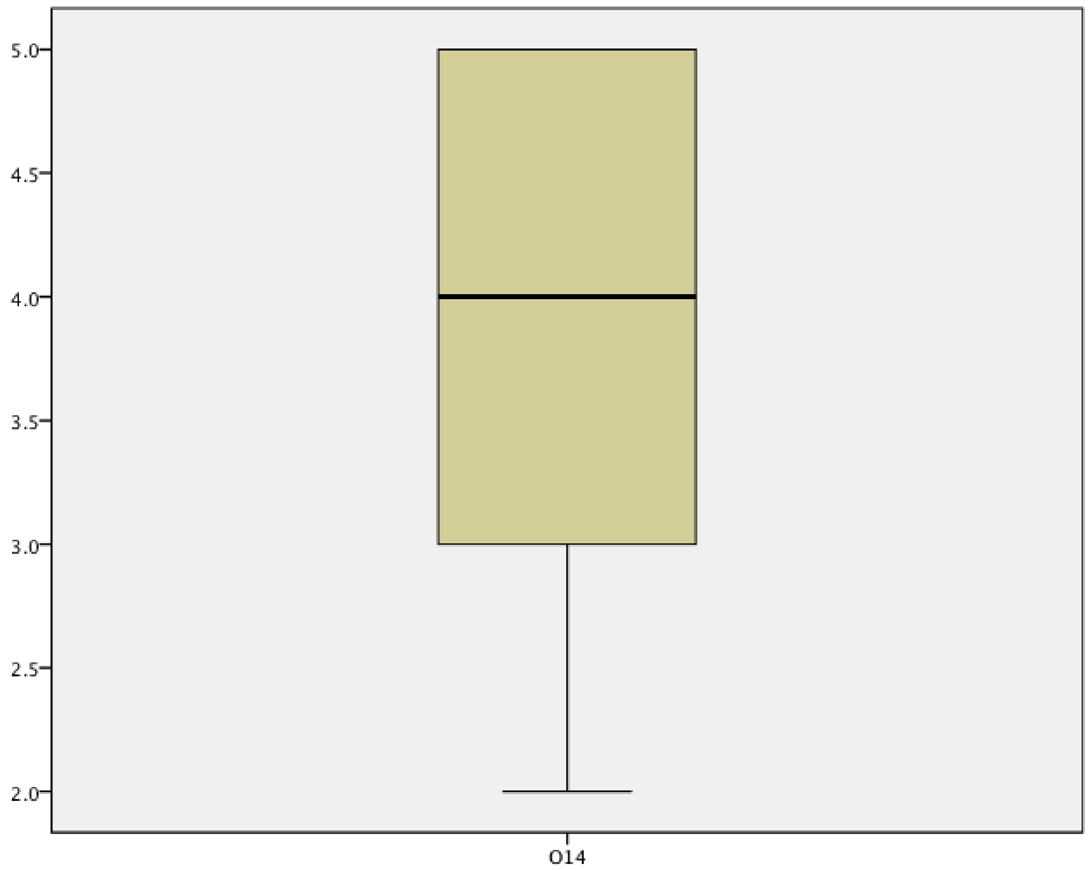


```
O13 Stem-and-Leaf Plot

 Frequency    Stem &  Leaf

    22.00        1 .  0000000000000000000000
      .00        1 .
      .00        1 .
      .00        1 .
      .00        1 .
    27.00        2 .  000000000000000000000000000
      .00        2 .
      .00        2 .
      .00        2 .
      .00        2 .
    46.00        3 .  0000000000000000000000000000000000000000000000
      .00        3 .
      .00        3 .
      .00        3 .
      .00        3 .
    13.00        4 .  0000000000000
     2.00 Extremes    (>=5)

 Stem width:  1
 Each leaf:        1 case(s)
```

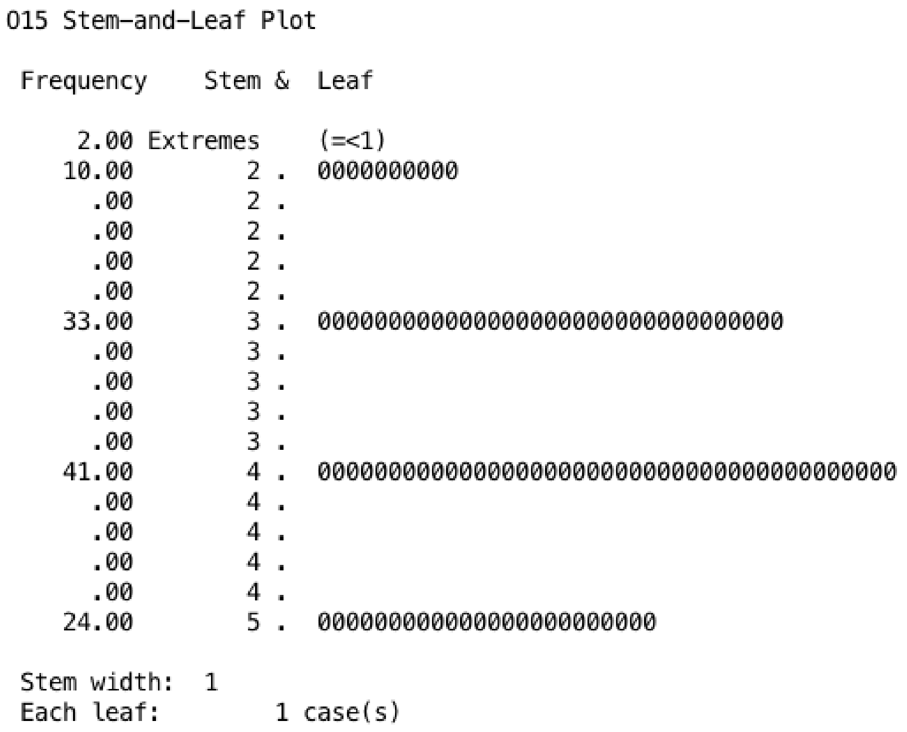


Variable O14

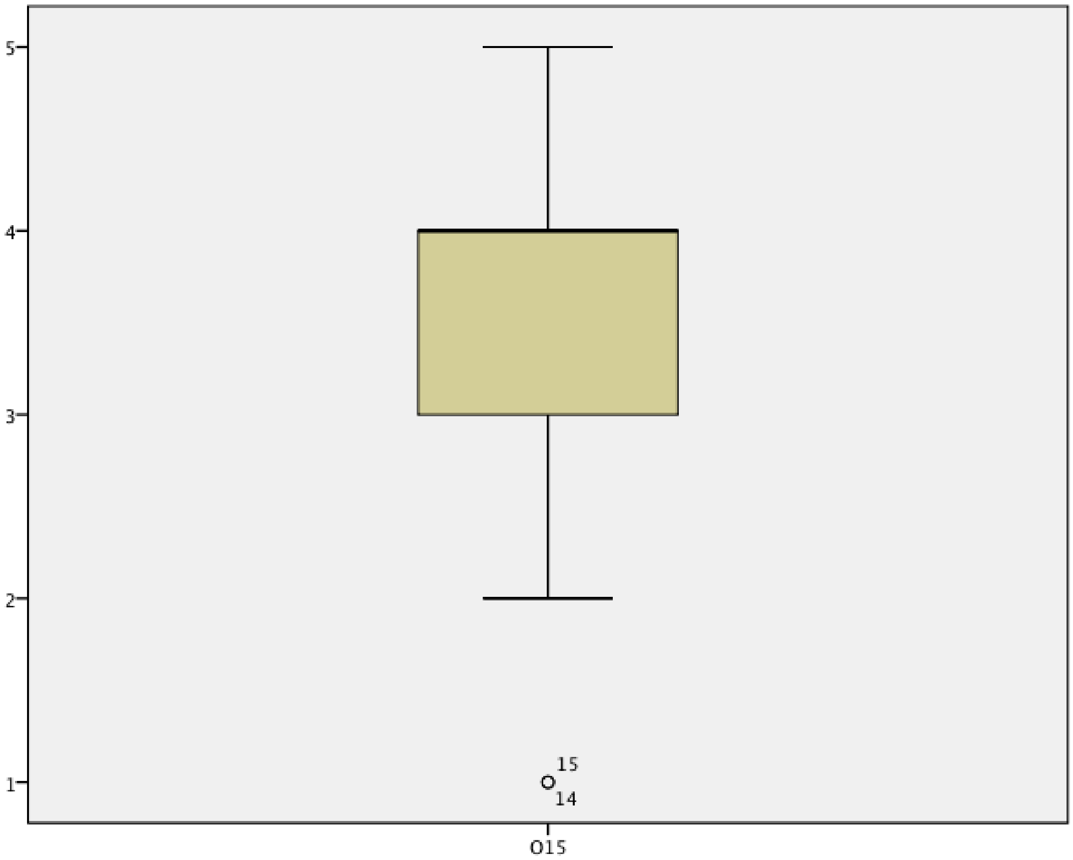
```
 O14 Stem-and-Leaf Plot

  Frequency    Stem &  Leaf

      4.00        2 .  0000
       .00        2 .
       .00        2 .
       .00        2 .
       .00        2 .
     24.00        3 .  000000000000000000000000
       .00        3 .
       .00        3 .
       .00        3 .
       .00        3 .
     28.00        4 .  0000000000000000000000000000
       .00        4 .
       .00        4 .
       .00        4 .
       .00        4 .
     54.00        5 .  000000000000000000000000000000000000000000000000000000

  Stem width:   1
  Each leaf:        1 case(s)
```



Variable O15

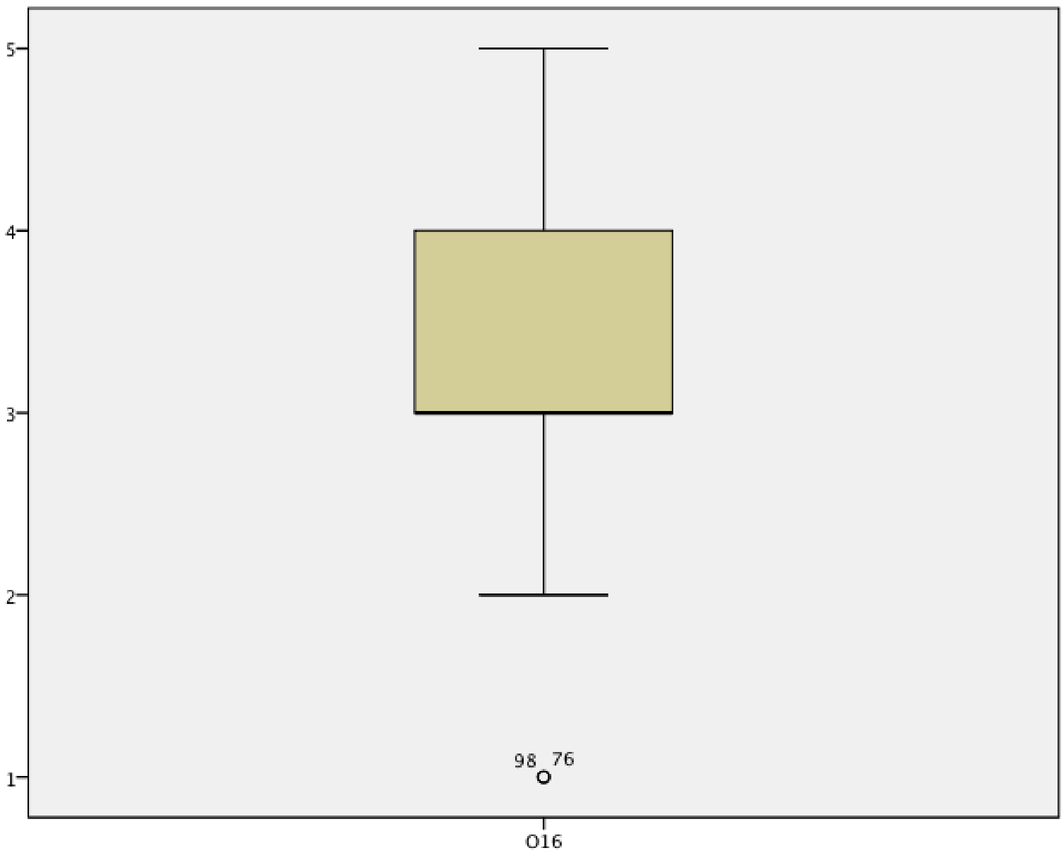


```
O15 Stem-and-Leaf Plot

 Frequency    Stem &  Leaf

     2.00 Extremes    (=<1)
    10.00        2 .  0000000000
      .00        2 .
      .00        2 .
      .00        2 .
      .00        2 .
    33.00        3 .  000000000000000000000000000000000
      .00        3 .
      .00        3 .
      .00        3 .
      .00        3 .
    41.00        4 .  00000000000000000000000000000000000000000
      .00        4 .
      .00        4 .
      .00        4 .
      .00        4 .
    24.00        5 .  000000000000000000000000

 Stem width:  1
 Each leaf:        1 case(s)
```

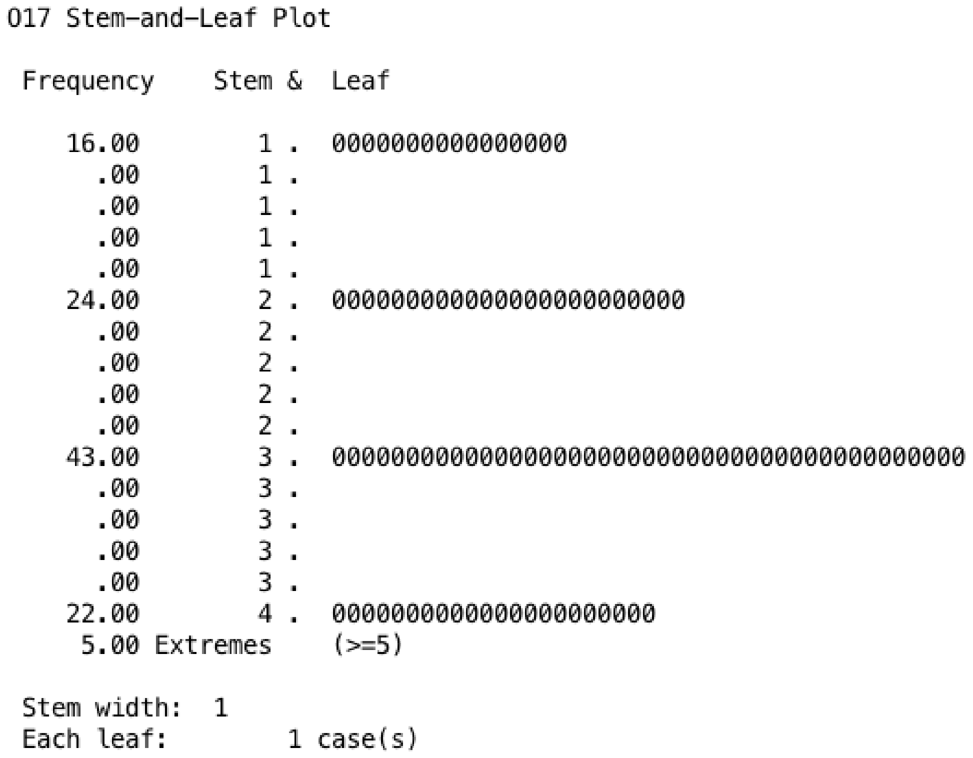


Variable O16

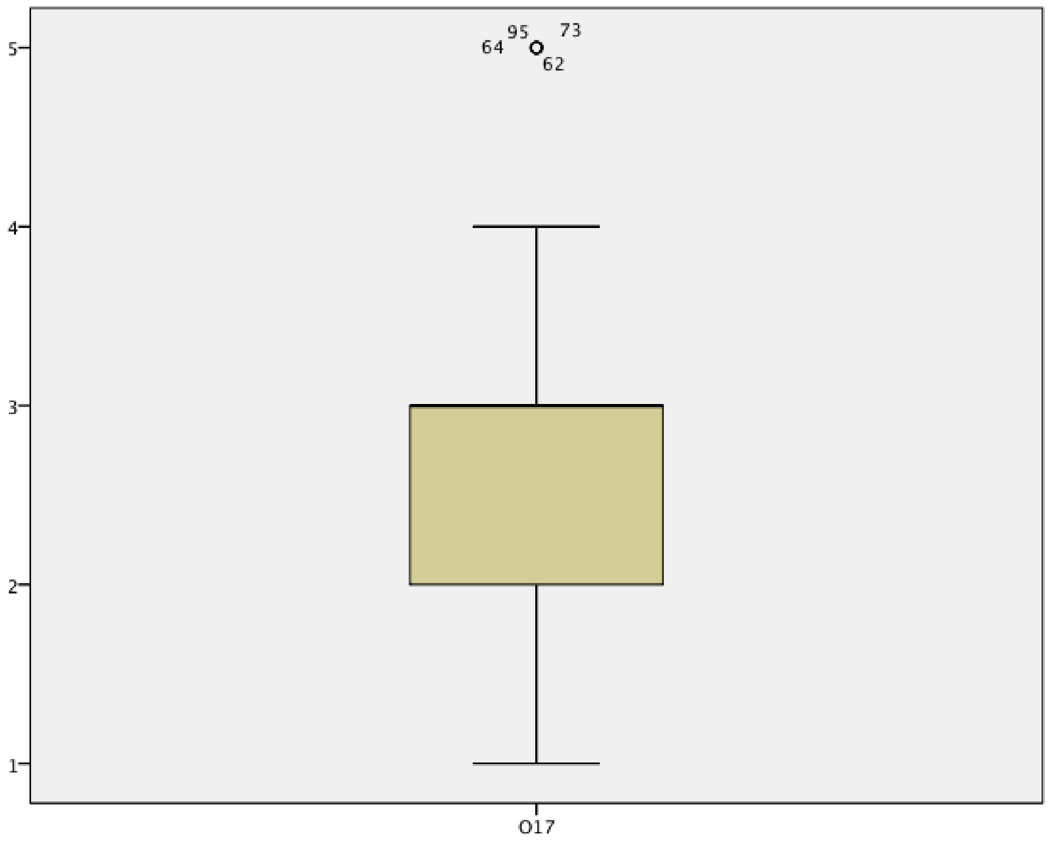
```
O16 Stem-and-Leaf Plot

 Frequency    Stem &  Leaf

     3.00 Extremes    (=<1)
    19.00        2 .  0000000000000000000
      .00        2 .
      .00        2 .
      .00        2 .
      .00        2 .
    52.00        3 .  0000000000000000000000000000000000000000000000000000
      .00        3 .
      .00        3 .
      .00        3 .
      .00        3 .
    25.00        4 .  0000000000000000000000000
      .00        4 .
      .00        4 .
      .00        4 .
      .00        4 .
    11.00        5 .  00000000000

 Stem width:  1
 Each leaf:        1 case(s)
```



Variable O17



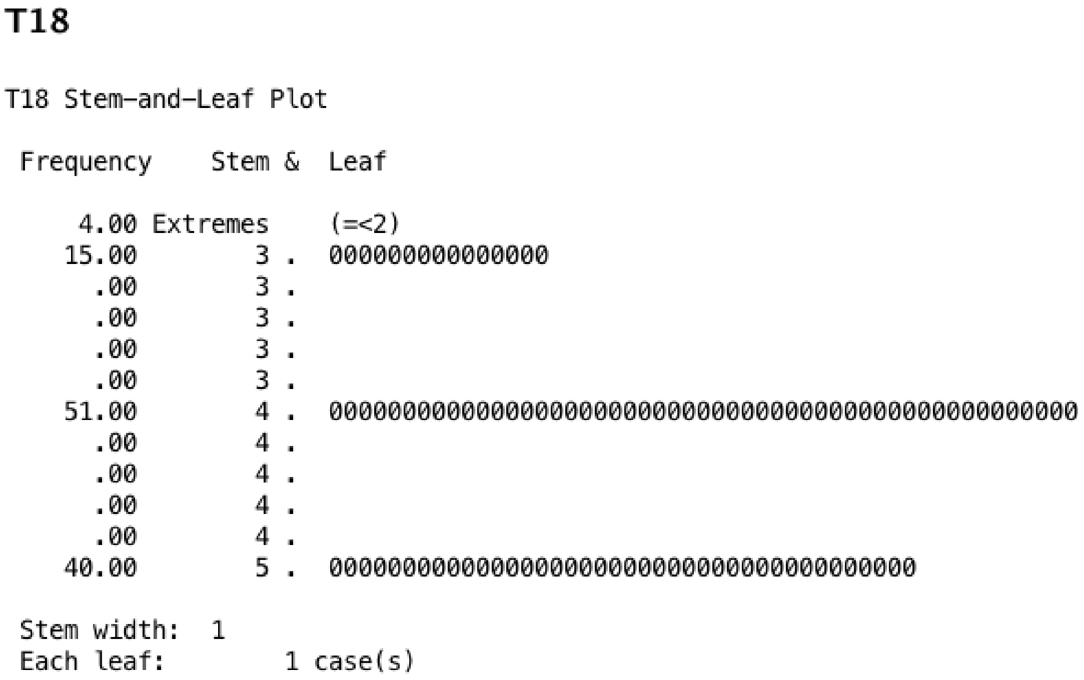
```
O17 Stem-and-Leaf Plot

 Frequency    Stem &  Leaf

    16.00        1 .  0000000000000000
      .00        1 .
      .00        1 .
      .00        1 .
      .00        1 .
    24.00        2 .  000000000000000000000000
      .00        2 .
      .00        2 .
      .00        2 .
      .00        2 .
    43.00        3 .  0000000000000000000000000000000000000000000
      .00        3 .
      .00        3 .
      .00        3 .
      .00        3 .
    22.00        4 .  0000000000000000000000
     5.00 Extremes    (>=5)

 Stem width:  1
 Each leaf:        1 case(s)
```



Technological Factors

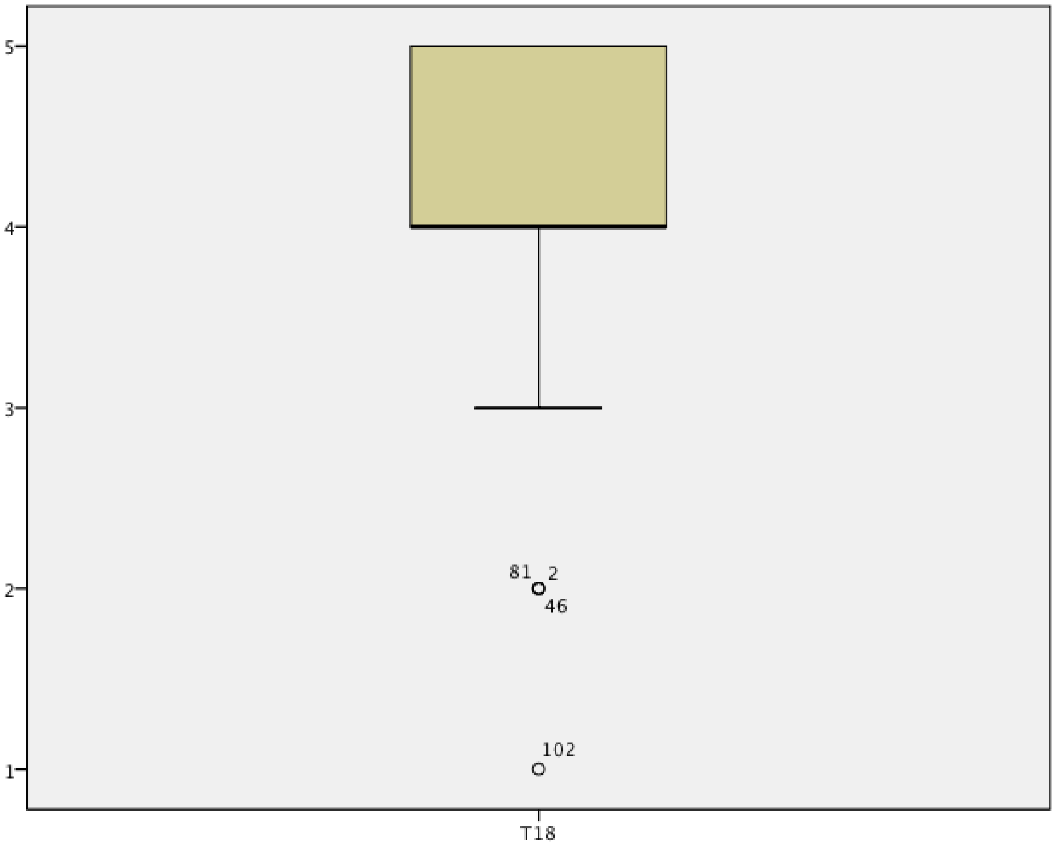
Outliers were identified in the results for seven of the technological factor variables. The diagram below presents the stem and leaf output and box plot highlighting the outlier from SPSS.

Variable T18



T18

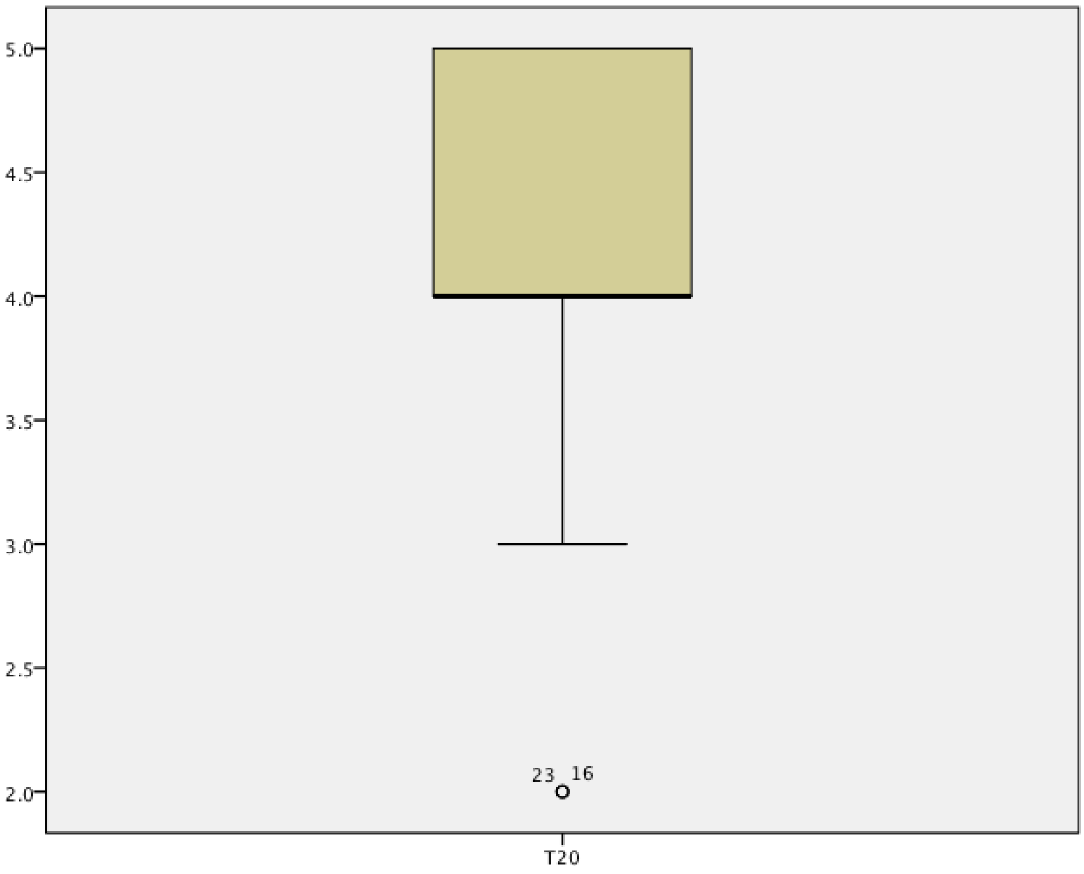
```
T18 Stem-and-Leaf Plot

 Frequency    Stem &  Leaf

     4.00 Extremes    (=<2)
    15.00        3 .  000000000000000
      .00        3 .
      .00        3 .
      .00        3 .
      .00        3 .
    51.00        4 .  000000000000000000000000000000000000000000000000000
      .00        4 .
      .00        4 .
      .00        4 .
      .00        4 .
    40.00        5 .  0000000000000000000000000000000000000000

 Stem width:  1
 Each leaf:        1 case(s)
```



Variable T20

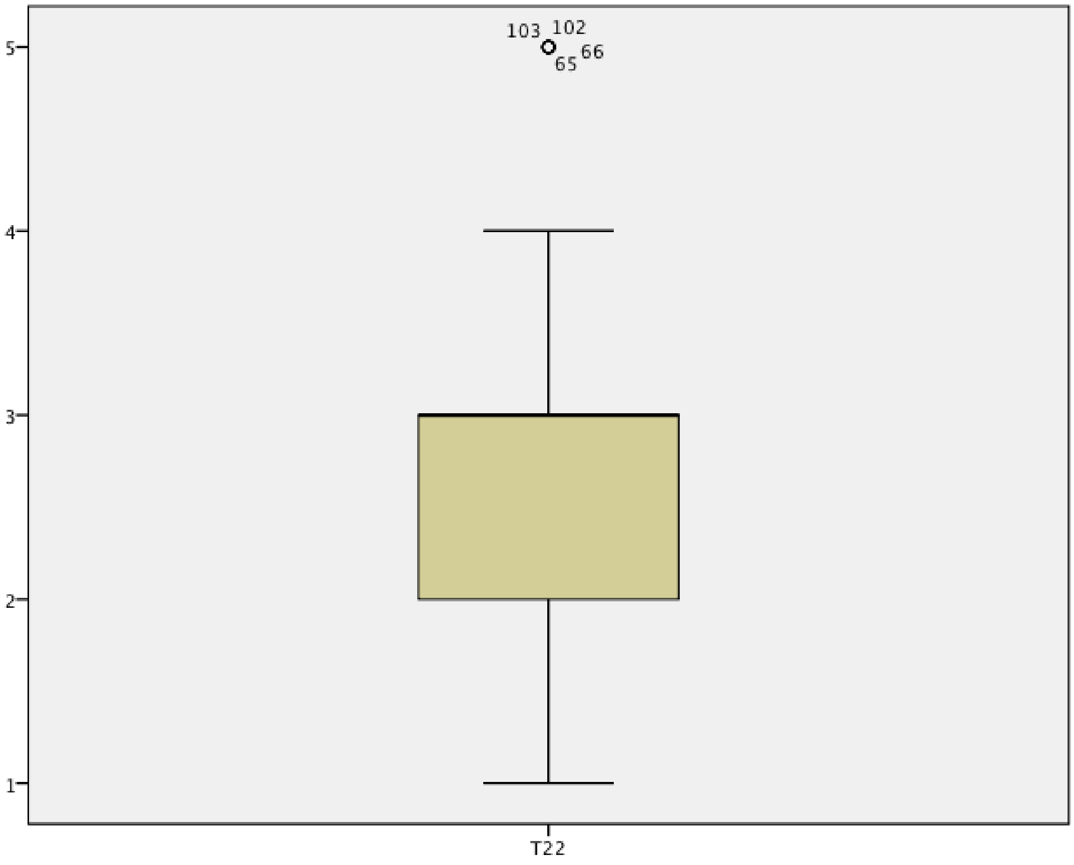
T20

```
T20 Stem-and-Leaf Plot

 Frequency    Stem &  Leaf

     3.00 Extremes    (=<2)
    18.00        3 .  000000000000000000
      .00        3 .
      .00        3 .
      .00        3 .
      .00        3 .
    53.00        4 .  00000000000000000000000000000000000000000000000000000
      .00        4 .
      .00        4 .
      .00        4 .
      .00        4 .
    36.00        5 .  000000000000000000000000000000000000

 Stem width:   1
 Each leaf:        1 case(s)
```

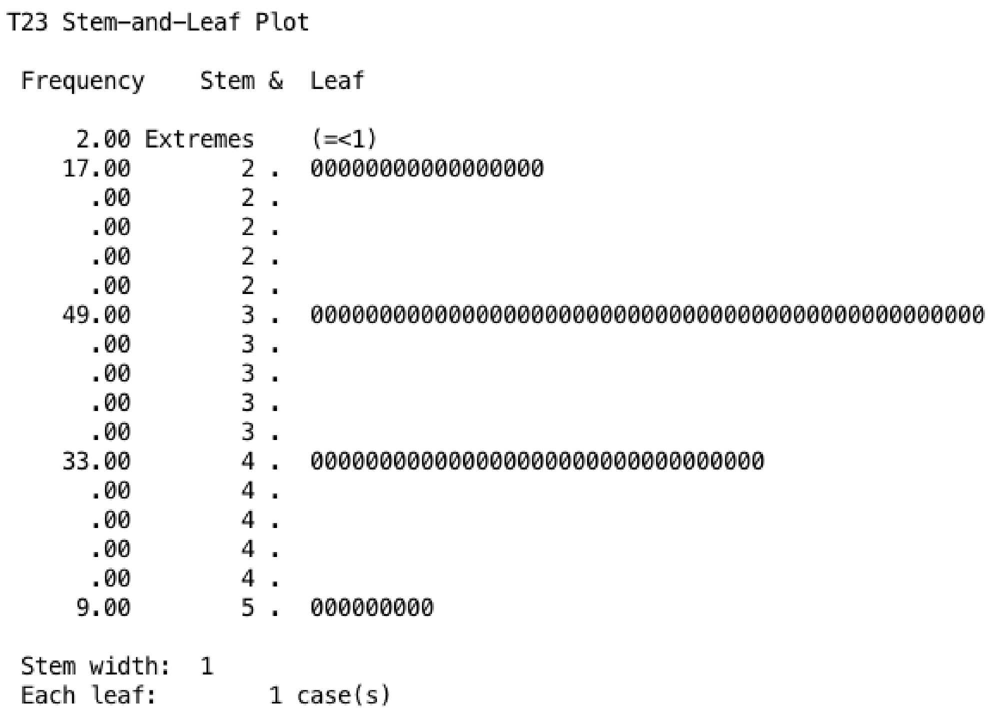


Variable T22

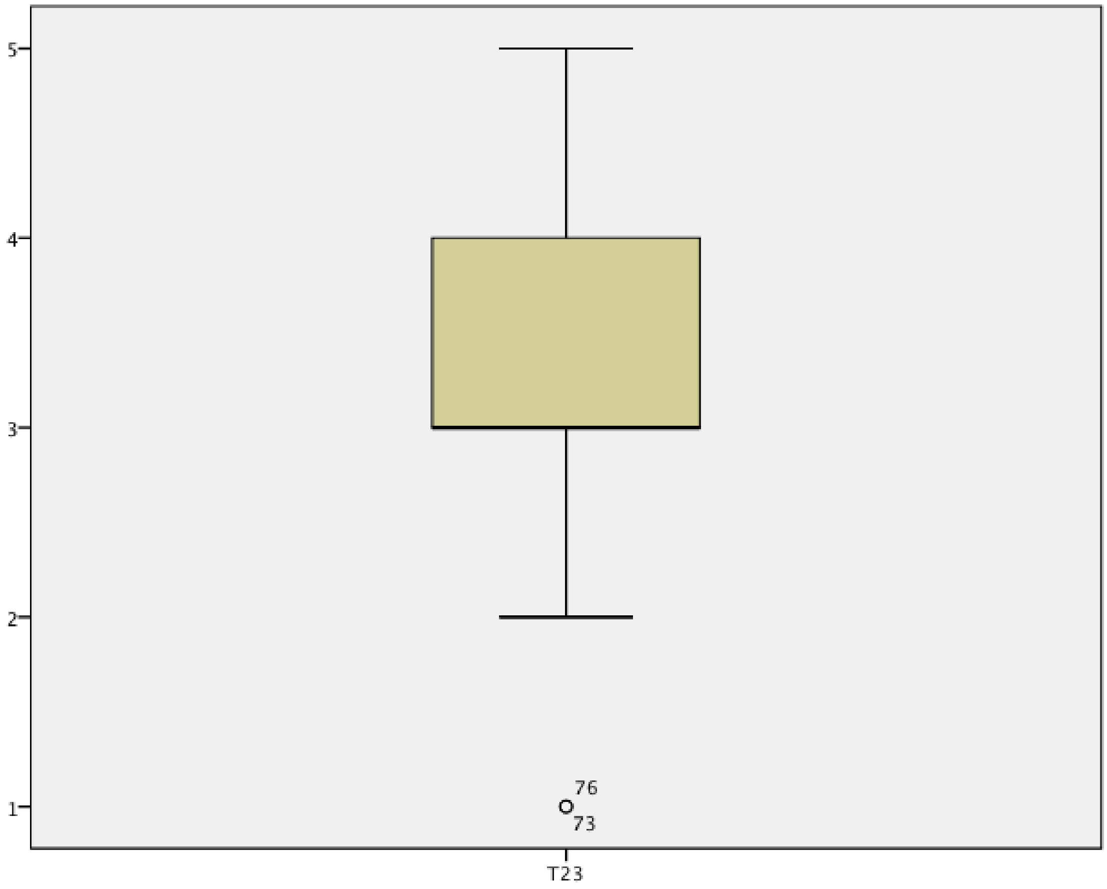
```
T22 Stem-and-Leaf Plot

 Frequency    Stem &  Leaf

    17.00        1 .  00000000000000000
      .00        1 .
      .00        1 .
      .00        1 .
      .00        1 .
    35.00        2 .  00000000000000000000000000000000000
      .00        2 .
      .00        2 .
      .00        2 .
      .00        2 .
    41.00        3 .  00000000000000000000000000000000000000000
      .00        3 .
      .00        3 .
      .00        3 .
      .00        3 .
     9.00        4 .  000000000
     8.00 Extremes    (>=5)

 Stem width:  1
 Each leaf:        1 case(s)
```



Variable T23

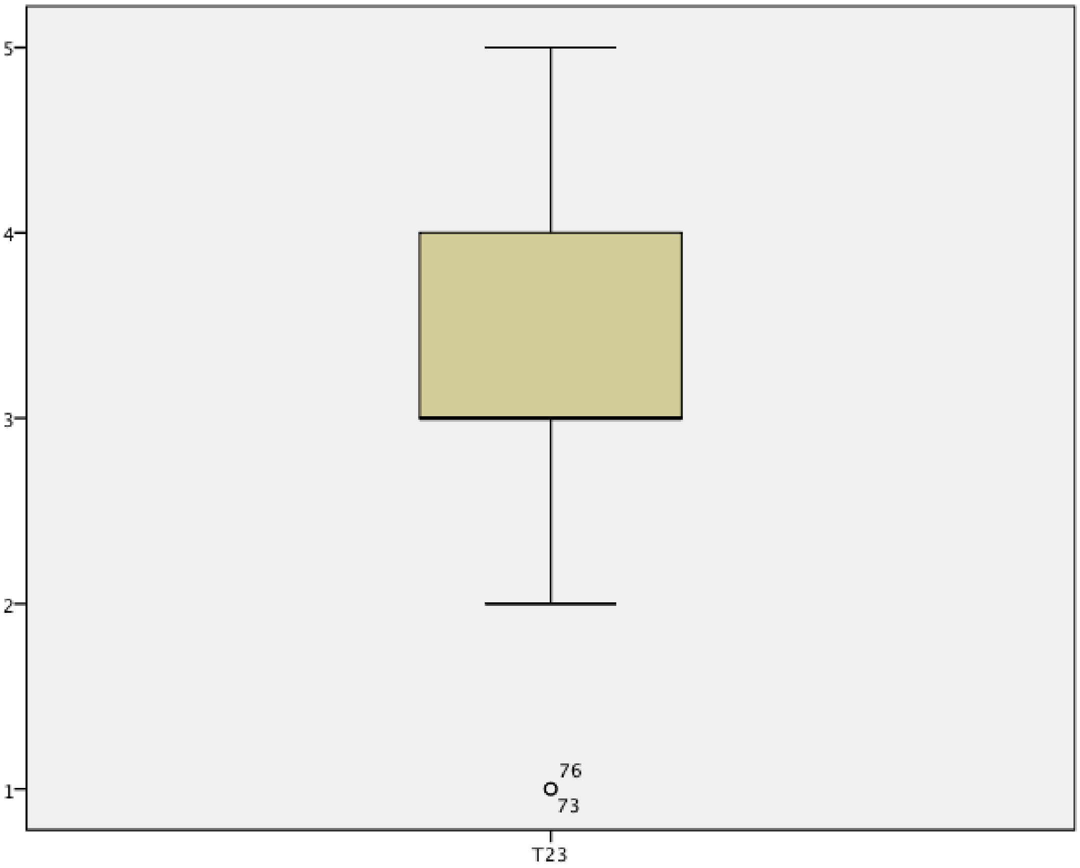


```
T23 Stem-and-Leaf Plot

 Frequency    Stem &  Leaf

     2.00 Extremes    (=<1)
    17.00        2 .  00000000000000000
      .00        2 .
      .00        2 .
      .00        2 .
      .00        2 .
    49.00        3 .  0000000000000000000000000000000000000000000000000
      .00        3 .
      .00        3 .
      .00        3 .
      .00        3 .
    33.00        4 .  000000000000000000000000000000000
      .00        4 .
      .00        4 .
      .00        4 .
      .00        4 .
     9.00        5 .  000000000

 Stem width:  1
 Each leaf:        1 case(s)
```



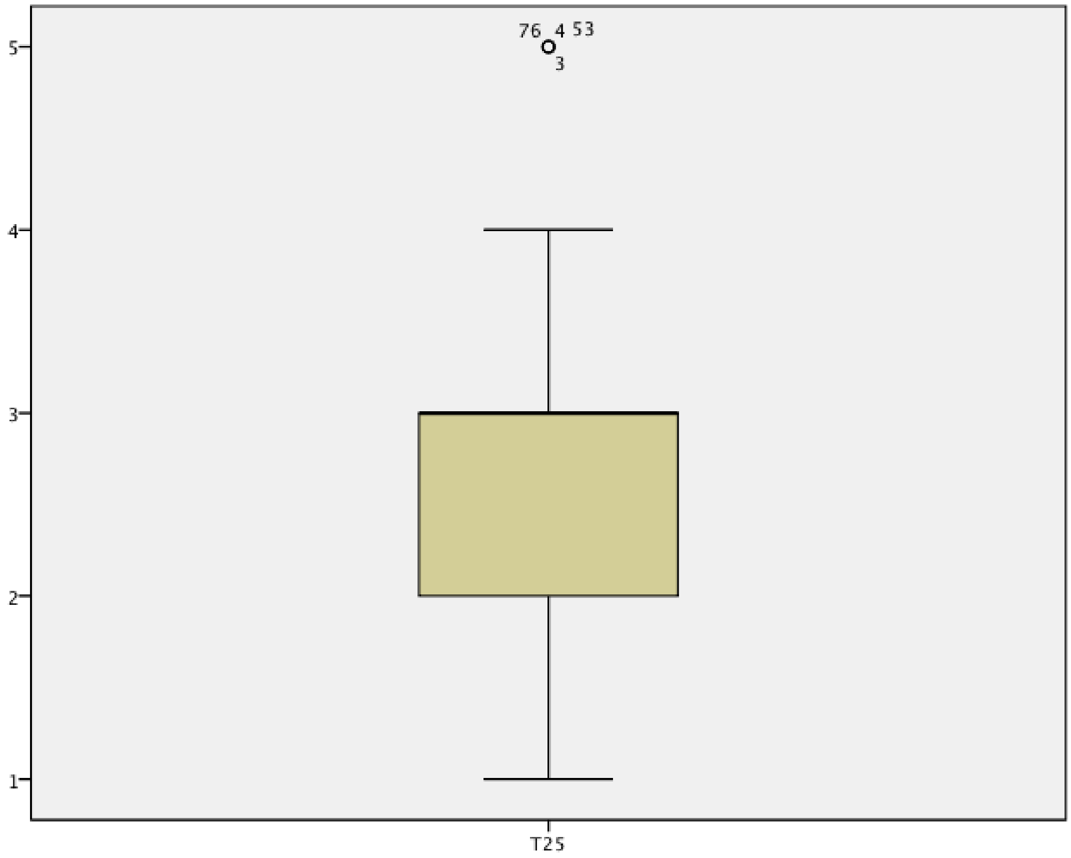
Variable T24

```
T24 Stem-and-Leaf Plot

 Frequency    Stem &  Leaf

     4.00 Extremes    (=<2)
    15.00        3 .  000000000000000
      .00        3 .
      .00        3 .
      .00        3 .
      .00        3 .
    62.00        4 .  00000000000000000000000000000000000000000000000000000000000000
      .00        4 .
      .00        4 .
      .00        4 .
      .00        4 .
    29.00        5 .  00000000000000000000000000000

 Stem width:  1
 Each leaf:        1 case(s)
```



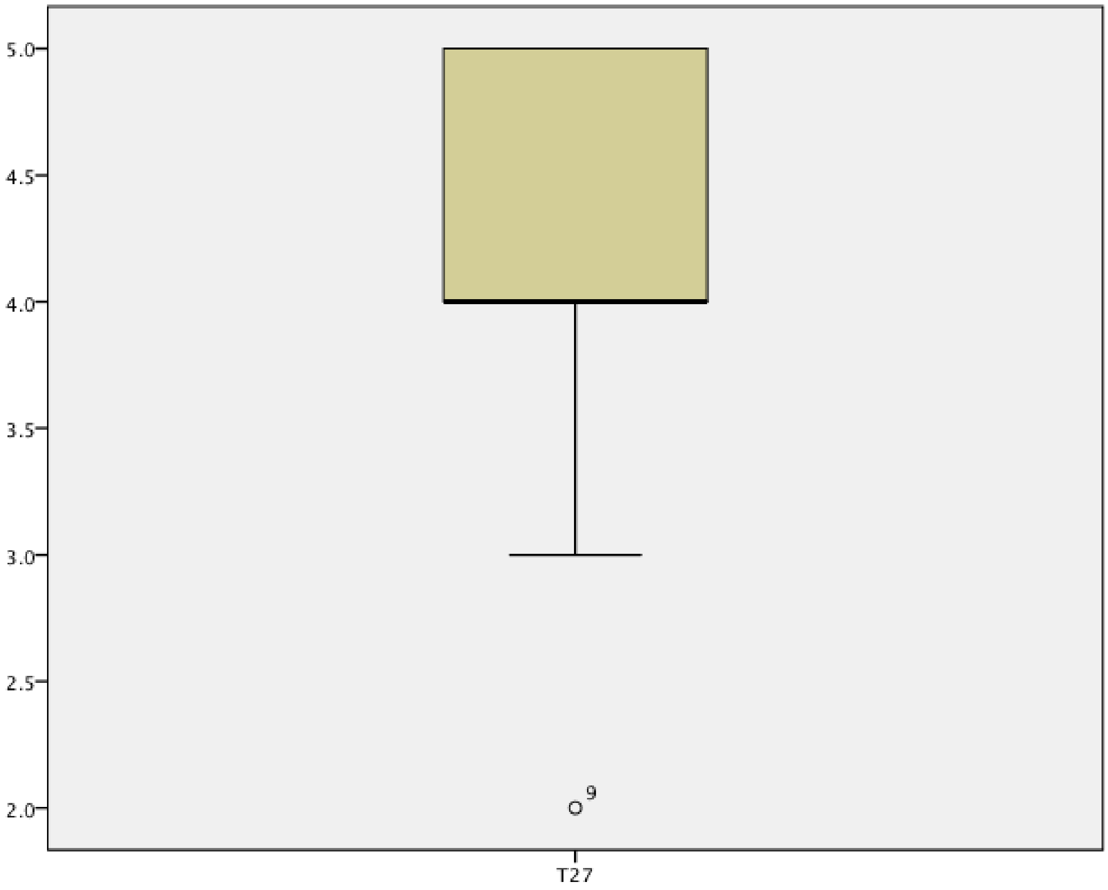
Variable T25

```
T25 Stem-and-Leaf Plot

 Frequency    Stem &  Leaf

    18.00        1 .  000000000000000000
      .00        1 .
      .00        1 .
      .00        1 .
      .00        1 .
    33.00        2 .  000000000000000000000000000000000
      .00        2 .
      .00        2 .
      .00        2 .
      .00        2 .
    34.00        3 .  0000000000000000000000000000000000
      .00        3 .
      .00        3 .
      .00        3 .
      .00        3 .
    21.00        4 .  000000000000000000000
     4.00 Extremes    (>=5)

 Stem width:   1
 Each leaf:        1 case(s)
```



Variable T27

```
T27 Stem-and-Leaf Plot

 Frequency    Stem &  Leaf

     1.00 Extremes    (=<2)
    17.00        3 .  00000000000000000
      .00        3 .
      .00        3 .
      .00        3 .
      .00        3 .
    41.00        4 .  00000000000000000000000000000000000000000
      .00        4 .
      .00        4 .
      .00        4 .
      .00        4 .
    51.00        5 .  000000000000000000000000000000000000000000000000000

 Stem width:   1
 Each leaf:        1 case(s)
```



APPENDIX F: Non-Response Bias Analysis

Test Statistics[a] - Strategic Factors

	S1	S2	S3	S4	S5	S6	S7	S8
Mann-Whitney U	1305.500	1357.000	1387.500	1150.500	1281.500	1226.500	1317.500	1332.000
Wilcoxon W	3720.500	2218.000	3802.500	3565.500	3696.500	3641.500	2178.500	2193.000
Z	-.705	-.374	-.174	-1.722	-.899	-1.234	-.632	-.567
Asymp. Sig. (2-tailed)	.481	.708	.862	.085	.368	.217	.527	.571

a. Grouping Variable: Response_Wave

Test Statistics[a] - Operational Factors

	O9	O10	O11	O12	O13	O14	O15	O16	O17
Mann-Whitney U	1336.500	1400.000	1395.000	1148.000	1330.500	1346.500	1232.000	1414.500	1356.500
Wilcoxon W	3751.500	3815.000	3810.000	3563.000	3745.500	3761.500	3647.000	2275.500	3771.500
Z	-.524	-.098	-.127	-1.710	-.547	-.455	-1.183	.000	-.374
Asymp. Sig. (2-tailed)	.600	.922	.899	.087	.585	.649	.237	1.000	.708

a. Grouping Variable: Response_Wave

Test Statistics[a] - Technological Factors

	T18	T19	T20	T21	T22	T23	T24	T25	T26	T27	T28
Mann-Whitney U	1357.000	1360.000	1313.500	1307.000	1403.500	1286.000	1299.000	1345.500	1360.500	1400.000	1286.000
Wilcoxon W	3772.000	3775.000	3728.500	2168.000	2264.500	3701.000	2160.000	3760.500	2221.500	3815.000	3701.000
Z	-.386	-.353	-.678	-.728	-.071	-.847	-.798	-.442	-.349	-.098	-.822
Asymp. Sig. (2-tailed)	.700	.724	.498	.467	.943	.397	.425	.659	.727	.922	.411

a. Grouping Variable: Response_Wave

APPENDIX G: Common Method Bias Analysis

Total Variance Explained

	Initial Eigenvalues			Extraction Sums of Squared Loadings		
Component	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	3.305	11.805	11.805	3.305	11.805	11.805
2	2.691	9.611	21.416			
3	2.125	7.590	29.006			
4	1.991	7.111	36.117			
5	1.686	6.021	42.138			
6	1.651	5.898	48.035			
7	1.360	4.858	52.893			
8	1.233	4.403	57.296			
9	1.131	4.040	61.336			
10	1.113	3.974	65.310			
11	.971	3.467	68.777			
12	.892	3.185	71.962			
13	.857	3.061	75.023			
14	.787	2.812	77.834			
15	.761	2.719	80.554			
16	.718	2.565	83.119			
17	.637	2.274	85.393			
18	.615	2.196	87.589			
19	.560	1.999	89.588			
20	.511	1.824	91.411			
21	.433	1.547	92.959			
22	.406	1.449	94.408			
23	.351	1.254	95.662			
24	.311	1.110	96.772			
25	.287	1.025	97.797			
26	.260	.930	98.727			
27	.206	.735	99.462			
28	.151	.538	100.000			

Extraction Method: Principal Component Analysis.

APPENDIX H: Spearman’s Correlation Analysis

Correlations – Strategic Factors

			S1	S2	S3	S4	S5	S6	S7	S8
Spearman's rho	S1	Correlation Coefficient	1.000	.188*	.098	-.124	.250**	.245**	.002	.253**
		Sig. (2-tailed)	.	.050	.311	.198	.008	.010	.981	.008
		N	110	110	110	110	110	110	110	110
	S2	Correlation Coefficient	.188*	1.000	-.095	-.087	.289**	.304**	-.063	.248**
		Sig. (2-tailed)	.050	.	.322	.368	.002	.001	.512	.009
		N	110	110	110	110	110	110	110	110
	S3	Correlation Coefficient	.098	-.095	1.000	.317**	.162	-.014	.264**	.050
		Sig. (2-tailed)	.311	.322	.	.001	.091	.881	.005	.603
		N	110	110	110	110	110	110	110	110
	S4	Correlation Coefficient	-.124	-.087	.317**	1.000	.138	-.033	.102	-.123
		Sig. (2-tailed)	.198	.368	.001	.	.149	.729	.290	.200
		N	110	110	110	110	110	110	110	110
	S5	Correlation Coefficient	.250**	.289**	.162	.138	1.000	.303**	.002	.208*
		Sig. (2-tailed)	.008	.002	.091	.149	.	.001	.983	.029
		N	110	110	110	110	110	110	110	110
	S6	Correlation Coefficient	.245**	.304**	-.014	-.033	.303**	1.000	.054	.221*
		Sig. (2-tailed)	.010	.001	.881	.729	.001	.	.572	.020
		N	110	110	110	110	110	110	110	110
	S7	Correlation Coefficient	.002	-.063	.264**	.102	.002	.054	1.000	.144
		Sig. (2-tailed)	.981	.512	.005	.290	.983	.572	.	.134
		N	110	110	110	110	110	110	110	110
	S8	Correlation Coefficient	.253**	.248**	.050	-.123	.208*	.221*	.144	1.000
		Sig. (2-tailed)	.008	.009	.603	.200	.029	.020	.134	.
		N	110	110	110	110	110	110	110	110

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

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

Correlations – Operational Factors

			O9	O10	O11	O12	O13	O14	O15	O16	O17
Spearman's rho	O9	Correlation Coefficient	1.000	.263**	.392**	.264**	-.103	.376**	.172	-.085	.172
		Sig. (2-tailed)	.	.005	.000	.005	.285	.000	.073	.377	.073
		N	110	110	110	110	110	110	110	110	110
	O10	Correlation Coefficient	.263**	1.000	.113	.047	.024	.181	.204*	-.124	-.038
		Sig. (2-tailed)	.005	.	.241	.623	.805	.058	.032	.197	.693
		N	110	110	110	110	110	110	110	110	110
	O11	Correlation Coefficient	.392**	.113	1.000	.309**	-.155	.196*	.052	-.083	.230*
		Sig. (2-tailed)	.000	.241	.	.001	.106	.041	.592	.388	.016
		N	110	110	110	110	110	110	110	110	110
	O12	Correlation Coefficient	.264**	.047	.309**	1.000	-.008	.175	.196*	-.031	.206*
		Sig. (2-tailed)	.005	.623	.001	.	.935	.068	.041	.745	.031
		N	110	110	110	110	110	110	110	110	110
	O13	Correlation Coefficient	-.103	.024	-.155	-.008	1.000	.027	.254**	.352**	.118
		Sig. (2-tailed)	.285	.805	.106	.935	.	.782	.007	.000	.219
		N	110	110	110	110	110	110	110	110	110
	O14	Correlation Coefficient	.376**	.181	.196*	.175	.027	1.000	.157	.121	.011
		Sig. (2-tailed)	.000	.058	.041	.068	.782	.	.102	.209	.910
		N	110	110	110	110	110	110	110	110	110
	O15	Correlation Coefficient	.172	.204*	.052	.196*	.254**	.157	1.000	.272**	.187
		Sig. (2-tailed)	.073	.032	.592	.041	.007	.102	.	.004	.050
		N	110	110	110	110	110	110	110	110	110
	O16	Correlation Coefficient	-.085	-.124	-.083	-.031	.352**	.121	.272**	1.000	.128

		Sig. (2-tailed)	.377	.197	.388	.745	.000	.209	.004	.	.182
		N	110	110	110	110	110	110	110	110	110
	O17	Correlation Coefficient	.172	-.038	.230*	.206*	.118	.011	.187	.128	1.000
		Sig. (2-tailed)	.073	.693	.016	.031	.219	.910	.050	.182	.
		N	110	110	110	110	110	110	110	110	110

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

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

Correlations – Technological Factors

			T18	T19	T20	T21	T22	T23	T24	T25	T26	T27	T28
Spearman's rho	T18	Correlation Coefficient	1.000	.234*	.223*	.184	.051	.197*	.248**	.067	.061	.225*	.180
		Sig. (2-tailed)	.	.014	.019	.054	.597	.039	.009	.487	.524	.018	.060
		N	110	110	110	110	110	110	110	110	110	110	110
	T19	Correlation Coefficient	.234*	1.000	.203*	.078	.074	.104	.096	-.073	.125	-.015	.047
		Sig. (2-tailed)	.014	.	.033	.418	.440	.278	.316	.449	.194	.878	.629
		N	110	110	110	110	110	110	110	110	110	110	110
	T20	Correlation Coefficient	.223*	.203*	1.000	.343**	.186	.296**	.113	-.043	-.019	.055	-.160
		Sig. (2-tailed)	.019	.033	.	.000	.051	.002	.240	.657	.841	.567	.095
		N	110	110	110	110	110	110	110	110	110	110	110
	T21	Correlation Coefficient	.184	.078	.343**	1.000	.286**	.260**	.131	.095	.036	.091	.061
		Sig. (2-tailed)	.054	.418	.000	.	.002	.006	.173	.326	.711	.347	.527

		N	110	110	110	110	110	110	110	110	110	110	110
	T22	Correlation Coefficient	.051	.074	.186	.286**	1.000	.597**	.069	.126	.150	-.023	.091
		Sig. (2-tailed)	.597	.440	.051	.002	.	.000	.476	.191	.117	.814	.343
		N	110	110	110	110	110	110	110	110	110	110	110
	T23	Correlation Coefficient	.197*	.104	.296**	.260**	.597**	1.000	.266**	-.009	.027	.107	-.011
		Sig. (2-tailed)	.039	.278	.002	.006	.000	.	.005	.924	.776	.268	.911
		N	110	110	110	110	110	110	110	110	110	110	110
	T24	Correlation Coefficient	.248**	.096	.113	.131	.069	.266**	1.000	.030	-.099	.019	.050
		Sig. (2-tailed)	.009	.316	.240	.173	.476	.005	.	.753	.301	.842	.604
		N	110	110	110	110	110	110	110	110	110	110	110
	T25	Correlation Coefficient	.067	-.073	-.043	.095	.126	-.009	.030	1.000	.541**	.162	.471**
		Sig. (2-tailed)	.487	.449	.657	.326	.191	.924	.753	.	.000	.091	.000
		N	110	110	110	110	110	110	110	110	110	110	110
	T26	Correlation Coefficient	.061	.125	-.019	.036	.150	.027	-.099	.541**	1.000	.137	.518**
		Sig. (2-tailed)	.524	.194	.841	.711	.117	.776	.301	.000	.	.153	.000
		N	110	110	110	110	110	110	110	110	110	110	110
	T27	Correlation Coefficient	.225*	-.015	.055	.091	-.023	.107	.019	.162	.137	1.000	.184
		Sig. (2-tailed)	.018	.878	.567	.347	.814	.268	.842	.091	.153	.	.054

		N	110	110	110	110	110	110	110	110	110	110	110
	T28	Correlation Coefficient	.180	.047	-.160	.061	.091	-.011	.050	.471**	.518**	.184	1.000
		Sig. (2-tailed)	.060	.629	.095	.527	.343	.911	.604	.000	.000	.054	.
		N	110	110	110	110	110	110	110	110	110	110	110

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

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

APPENDIX I: Mann-Whitney U Test

Test Statistics – Strategic Factors

	S1	S2	S3	S4	S5	S6	S7	S8
Mann-Whitney U	1155.000	1176.500	1319.000	1292.000	1054.500	1278.500	1248.000	1371.500
Wilcoxon W	2145.000	2166.500	2309.000	2282.000	3199.500	2268.500	2238.000	3516.500
Z	-1.786	-1.647	-.713	-.901	-2.533	-.993	-1.186	-.401
Asymp. Sig. (2-tailed)	.074	.100	.476	.368	.011	.321	.236	.688

Test Statistics – Operational Factors

	O9	O10	O11	O12	O13	O14	O15	O16	O17
Mann-Whitney U	1430.000	1346.000	1256.500	1210.500	1253.500	1428.500	1252.500	1218.000	1130.500
Wilcoxon W	3575.000	3491.000	2246.500	2200.500	3398.500	2418.500	2242.500	2208.000	2120.500
Z	.000	-.570	-1.130	-1.406	-1.148	-.010	-1.149	-1.396	-1.931
Asymp. Sig. (2-tailed)	1.000	.569	.259	.160	.251	.992	.251	.163	.053

Test Statistics – Technological Factors

	T18	T19	T20	T21	T22	T23	T24	T25	T26	T27	T28
Mann-Whitney U	1379.500	1303.000	1246.500	1296.000	1300.000	1360.500	1294.500	1355.000	1196.000	1323.500	1264.000
Wilcoxon W	3524.500	3448.000	2236.500	3441.000	3445.000	3505.500	3439.500	2345.000	2186.000	3468.500	2254.000
Z	-.338	-.822	-1.229	-.907	-.842	-.458	-.939	-.480	-1.510	-.715	-1.061
Asymp. Sig. (2-tailed)	.735	.411	.219	.364	.400	.647	.348	.631	.131	.475	.289

APPENDIX J: Kruskal-Wallis Test

Ranks – Strategic Factors

	Experience	N	Mean Rank
S1	1	13	45.50
	2	64	57.43
	3	30	55.20
	4	3	60.67
	Total	110	
S2	1	13	46.31
	2	64	57.61
	3	30	57.17
	4	3	33.67
	Total	110	
S3	1	13	46.85
	2	64	55.59
	3	30	58.82
	4	3	57.83
	Total	110	
S4	1	13	55.81
	2	64	53.03
	3	30	58.68
	4	3	75.00
	Total	110	
S5	1	13	38.50
	2	64	61.59
	3	30	51.67
	4	3	37.50
	Total	110	
S6	1	13	40.77
	2	64	55.09
	3	30	64.43
	4	3	38.83
	Total	110	
S7	1	13	48.62
	2	64	54.91
	3	30	59.50
	4	3	58.00
	Total	110	
S8	1	13	50.42

	2	64	57.82
	3	30	54.40
	4	3	39.00
	Total	110	

Test Statistics – Strategic Factors								
	S1	S2	S3	S4	S5	S6	S7	S8
Chi-Square	1.761	3.155	1.406	2.010	8.877	6.714	1.242	1.860
df	3	3	3	3	3	3	3	3
Asymp. Sig.	.624	.368	.704	.570	.031	.082	.743	.602

Ranks – Operational Factors			
	Experience	N	Mean Rank
O9	1	13	53.42
	2	64	56.10
	3	30	55.03
	4	3	56.33
	Total	110	
O10	1	13	52.81
	2	64	58.05
	3	30	51.25
	4	3	55.33
	Total	110	
O11	1	13	59.77
	2	64	56.16
	3	30	54.35
	4	3	34.33
	Total	110	
O12	1	13	56.96
	2	64	56.41
	3	30	54.67
	4	3	38.17
	Total	110	
O13	1	13	64.85
	2	64	55.59
	3	30	51.58
	4	3	52.17

	Total	110	
O14	1	13	58.27
	2	64	55.03
	3	30	54.73
	4	3	61.17
	Total	110	
O15	1	13	60.12
	2	64	57.80
	3	30	51.45
	4	3	27.00
	Total	110	
O16	1	13	42.65
	2	64	55.08
	3	30	60.68
	4	3	68.33
	Total	110	
O17	1	13	59.12
	2	64	55.91
	3	30	52.45
	4	3	61.67
	Total	110	

Test Statistics – Operational Factors

	O9	O10	O11	O12	O13	O14	O15	O16	O17
Chi-Square	.102	1.239	1.806	1.061	1.775	.262	3.826	3.876	.614
df	3	3	3	3	3	3	3	3	3
Asymp. Sig.	.992	.744	.614	.786	.620	.967	.281	.275	.893

Ranks – Technological Factors			
	Experience	N	Mean Rank
T18	1	13	47.88
	2	64	54.71
	3	30	58.50
	4	3	75.33
	Total	110	
T19	1	13	52.88
	2	64	51.02
	3	30	63.72
	4	3	80.17
	Total	110	
T20	1	13	52.81
	2	64	55.59
	3	30	56.92
	4	3	51.00
	Total	110	
T21	1	13	63.00
	2	64	54.33
	3	30	54.63
	4	3	56.67
	Total	110	
T22	1	13	59.23
	2	64	57.37
	3	30	49.42
	4	3	60.33
	Total	110	
T23	1	13	45.12
	2	64	60.10
	3	30	51.33
	4	3	44.00
	Total	110	
T24	1	13	44.92
	2	64	58.30
	3	30	54.62
	4	3	50.50
	Total	110	
T25	1	13	74.42
	2	64	54.59
	3	30	50.10

	4	3	46.83
	Total	110	
T26	1	13	76.31
	2	64	49.90
	3	30	57.80
	4	3	61.83
	Total	110	
T27	1	13	52.23
	2	64	57.20
	3	30	57.17
	4	3	16.67
	Total	110	
T28	1	13	66.04
	2	64	51.04
	3	30	58.38
	4	3	76.17
	Total	110	

Test Statistics – Technological Factors

	T18	T19	T20	T21	T22	T23	T24	T25	T26	T27	T28
Chi-Square	2.595	5.643	.250	.997	1.708	4.102	2.522	6.123	8.498	5.737	4.466
df	3	3	3	3	3	3	3	3	3	3	3
Asymp. Sig.	.458	.130	.969	.802	.635	.251	.471	.106	.037	.125	.215

APPENDIX K: PCA Output

KMO and Bartlett's Test – Strategic Factors

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.646
Bartlett's Test of Sphericity	Approx. Chi-Square	92.327
	df	28
	Sig.	.000

Total Variance Explained – Strategic Factors

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	2.066	25.828	25.828	2.066	25.828	25.828	2.028	25.344	25.344
2	1.559	19.489	45.317	1.559	19.489	45.317	1.450	18.126	43.470
3	1.019	12.738	58.055	1.019	12.738	58.055	1.167	14.585	58.055
4	.859	10.743	68.798						
5	.729	9.109	77.907						
6	.640	7.999	85.906						
7	.596	7.446	93.353						
8	.532	6.647	100.000						

KMO and Bartlett's Test – Operational Factors

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.640
Bartlett's Test of Sphericity	Approx. Chi-Square	131.158
	df	36
	Sig.	.000

Total Variance Explained – Operational Factors

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	2.236	24.839	24.839	2.236	24.839	24.839	1.737	19.305	19.305
2	1.673	18.585	43.424	1.673	18.585	43.424	1.693	18.817	38.122
3	1.198	13.311	56.735	1.198	13.311	56.735	1.291	14.344	52.466
4	.891	9.899	66.634	.891	9.899	66.634	1.275	14.168	66.634
5	.767	8.526	75.160						
6	.673	7.480	82.640						
7	.586	6.508	89.147						
8	.511	5.683	94.831						
9	.465	5.169	100.000						

KMO and Bartlett's Test – Technological Factors

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.617
Bartlett's Test of Sphericity	Approx. Chi-Square	235.790
	df	55
	Sig.	.000

Total Variance Explained – Technological Factors

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	2.464	22.398	22.398	2.464	22.398	22.398	2.089	18.993	18.993
2	1.977	17.971	40.369	1.977	17.971	40.369	1.940	17.633	36.625
3	1.384	12.584	52.953	1.384	12.584	52.953	1.497	13.611	50.237
4	1.030	9.368	62.321	1.030	9.368	62.321	1.329	12.085	62.321
5	.942	8.564	70.886						
6	.866	7.871	78.757						
7	.651	5.921	84.678						
8	.555	5.043	89.721						
9	.458	4.160	93.880						
10	.375	3.411	97.291						
11	.298	2.709	100.000						

APPENDIX L: Case Study Interview Guide

Question	Sample Probe / Further Questions
Organisation Background	
Which e-banking services does your bank offer?	• How long have you been offering such services?
Which of the services present the most issues when it comes to e-banking fraud	• Where have the major lapses in security occurred?
Kindly provide details of the key measures that your bank takes to mitigate the risk of e-banking fraud.	• Why do you believe that these measures have been successful? • How were these measures implemented in the bank?
Strategic Factor Questions	
How does your bank share knowledge on e-banking fraud prevention?	• What mediums?
To what extent are you satisfied with the knowledge sharing and fraud prevention resources available to your bank?	• What has works well when it comes to sharing knowledge for fraud prevention?
Operational Factor Questions	
Do you believe Top Management Support is critical for preventing e-banking fraud?	• If yes, how does your top management support e-banking fraud prevention. • Please give examples of how Top Management have supported fraud prevention in your bank.
How do you monitor the rate fraud over e-banking mediums	• How regular does this take place? Do you set targets? How often? • Who is responsible for reviewing fraud rates?
How have you adjusted your internal controls to improve e-banking fraud prevention?	• Give an example of some controls you have introduced to prevent fraud?
What role does internal audits play in e-banking fraud prevention?	• How regular do they take place? • Do you feel that the more regular they take place, the greater impact in e-banking fraud prevention?
What controls does your bank have in place to protect customers against identity theft?	• Have any e-banking fraud issues arisen relating to breach of the banks data security measures? • How did the bank respond to this?

Does your bank carry out penetration tests for its systems?	• What is the scope of the tests? • How are they done? • How often do they take place?
Has the Know Your Customer (KYC) initiative had any impact on fraud prevention?	• If Yes, what impact has the KYC project had on e-banking fraud prevention if any?
What other controls have been implemented to help minimise the risk of e-banking fraud?	• Which of these have been the most effective?
Technological Factor Questions	
How important is the financial cost of deploying authentication systems	• What criteria are used to select fraud prevention solutions?
Do you use biometric technology for authentication?	• If Yes, what technology has been adopted, how does it work? • What impact has it had?
How important do you feel authentication solutions are in preventing e-banking fraud?	• What factors did you consider before selecting authentication methods?
How does your bank maintain strong authentication for its e-banking services?	• What are the types of authentication used for access authentication and transactional authentication? • How many layers of authentication are used?
How has the PCI DSS compliant card management system helped prevent fraud?	• Why do you believe it had the effect it did? • How was it implemented?
How has the implementation of Europay MasterCard and Visa (EMV) affected e-banking fraud?	• Why do you believe it had the effect it did? • How was it implemented?
How significant a role has One Time Passwords (OTPs) played in preventing fraud?	• What types of OTP does your bank use? • At which stages of bank transactions are OTPs used?
Framework Review	
Findings from earlier phases of the research were used to propose an EBFP framework. To what extent do you agree with the framework?	• What is your view on the factors that have been identified as critical? • Has an appropriate grouping of CSF been adopted?
Closing Checklist 1. Request for copies of any documentation that can be shared 2. Identify other potential interviewees 3. Thank the participant for their participation	