Coventry University

DOCTOR OF PHILOSOPHY

Success factors influencing cyber security risk management implementation: the cases of large Nigerian organisations

Olaniran, Olukemi

Award date:
2022

Awarding institution:
Coventry University

Link to publication

General rights
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of this thesis for personal non-commercial research or study
- This thesis cannot be reproduced or quoted extensively from without first obtaining permission from the copyright holder(s)
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal

Take down policy
If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

Download date: 04. Jul. 2025

SUCCESS FACTORS INFLUENCING CYBER SECURITY RISK MANAGEMENT IMPLEMENTATION: THE CASES OF LARGE NIGERIAN ORGANISATIONS

By

OLUKEMI KEHINDE OLANIRAN

PhD

March 2022

SUCCESS FACTORS INFLUENCING CYBER SECURITY RISK MANAGEMENT IMPLEMENTATION: THE CASES OF LARGE NIGERIAN ORGANISATIONS

A Thesis submitted in partial fulfilment of the University's requirements for the degree of Doctor of Philosophy

March 2022

Certificate of Ethical Approval

Applicant:

Olukemi Olaniran

Project Title:

EVALUATION OF SUCCESS FACTORS OF CYBERSECURITY RISK MANAGEMENT (CSRM) IN THE NIGERIAN LARGE ORGANIZATIONS.

This is to certify that the above named applicant has completed the Coventry University Ethical Approval process and their project has been confirmed and approved as Medium Risk

Date of approval:

25 July 2019

Project Reference Number:

P92738

PhD Abstract

Cyber security risk management implementation success has become inevitable for business survival in the 21st century. The increasing challenges of managing cyber security risks, the elaborate mitigation activities and implementing cybersecurity measures in large Nigerian organisations have brought Cyber Security Risk Management (CSRM) implementation success to the fore in academics and practitioners' minds. Organisations are still unable to effectively manage these challenges due to the limited knowledge and failures of critical asset identification, valuation and loss estimation and the business case to invest adequately. Research on success factors for CSRM implementation is an under-researched area presented to facilitate the decision-making process towards CSRM implementation success in large organisations in Nigeria. The researcher's understanding to date demonstrates the lack of security models. It explores the need and the implications for successful CSRM implementation yet to be assessed in large organisations in Nigeria. Therefore, this study provides opportunities for relevant and innovative research and shows that it is of great significance to explore this subject among large organisations in Nigeria. The result leads to the successful implementation of CSRM.

Grounded in the socio-technical theory, this research advances and contributes significantly to the body of knowledge because it: examines and evaluates combined social and technical factors influencing CSRM implementation success in Nigeria, analyses and proposes the adoption of socio-technical success factors. In doing so, propose a model for CSRM success factors as a decision-making tool and a reference guide in large organisations. This research examined the success factors for CSRM implementation in Nigeria through a qualitative, interpretive, multi-case study research design. Data collection was from semi-structured interviews of thirty subject experts with relevant years of experience in four case organisations' research areas, organisational and public documents. A thematic analysis identified organisational factors to align CSRM implementation needs with organisational objectives with appropriate corporate governance structure and strategies. Comprehensive CSRM process factors enable cybersecurity policies, risk management processes and procedures with various technological tools and controls to engage, guide and influence disciplined people factors and CSRM implementation success efforts. Findings from four case organisations reveal that these factors led to more durable decisions that culminated in the successful implementation of CSRM within an enabling defined legal and political environment.

Acknowledgement

I acknowledge first God for the strength, grace, and courage to finish this study. I appreciate my supervisors, Dr Muhammad Kamal, Dr Rebwar Gharib and Dr Zilia Iskoujina, for their support and guidance throughout the process of this work. Special thanks to the go-to (Drs Rebwar and Zilia) in days of tears, sicknesses, accident and confusion for their moral, pastoral and academic support that saw me through. Appreciation extends to Dr Mahmood Shah (the former DoS) and the interviewees for their time and expertise in supporting this study. I recognise the staff, colleagues at Coventry University and friends for their support. The final special thanks to my husband and children for their immense support, motivation and understanding throughout the process.

Declarations

This thesis provides an account of the study conducted by Olukemi Kehinde Olaniran.

Table of Contents

Participant No.

INFORMED CONSENT FORM:
Evaluation of success factors for cybersecurity risk management in large organisations in Nigeria

You are invited to take part in this research study for the purpose of collecting data on the evaluation of success factors for cybersecurity risk management (CSRM) in the large organisations in Nigeria.

Before you decide to take part, you must **read the accompanying Participant Information Sheet.**

Please do not hesitate to ask questions if anything is unclear or if you would like more information about any aspect of this research. It is important that you feel able to take the necessary time to decide whether or not you wish to take part.

If you are happy to participate, please confirm your consent by circling YES against each of the below statements and then signing and dating the form as participant.

1	**I confirm that I have read and understood the Participant Information Sheet for the above study and have had the opportunity to ask questions**	**YES**	**NO**
2	**I understand my participation is voluntary and that I am free to withdraw my data, without giving a reason, by contacting the lead researcher and the Research Support Office at any time until the date specified in the Participant Information Sheet**	**YES**	**NO**
3	**I have noted down my participant number (top left of this Consent Form) which may be required by the lead researcher if I wish to withdraw from the study**	**YES**	**NO**
4	**I understand that all the information I provide will be held securely and treated confidentially**	**YES**	**NO**
5	**I am happy for the information I provide to be used (anonymously) in academic papers and other formal research outputs**	**YES**	**NO**
6	**I am happy for the interview to be audio recorded**	**YES**	**NO**
7	**I agree to take part in the above study**	**YES**	**NO**

Thank you for your participation in this study. Your help is very much appreciated.

Participant's Name	**Date**	**Signature**
Researcher	**Date**	**Signature**
Olukemi	**Olaniran**	

Coventry University

List of Figures

List of Tables

Chapter 1: Introduction to the Research Area

1.1 Introduction

Cyber Security Risk Management (CSRM) has become a global phenomenon as organisations, individuals, and nations have witnessed more focused cyber security threats and sophistication of data breaches, a consistent trend over the last decade (Spremić and Šimunic 2018). Literature reports that Nigeria is a nation not spared by the stigma of the cybercrime industry (Wang, Nnaji and Jung 2020; Makeri 2017) and heartache of an alarming rate of cybersecurity and cyber-attacks heavily dependent on a complex network of interdependent factors (Abdul-Rasheed et al. 2016; Ajah and Chukwuemeka 2019).

Large organisations in Nigeria are becoming more cyber security conscious by implementing risk management initiatives for the protection and security monitoring measures (Aladenusi 2020; CBN 2018). Despite the extensive efforts, risk management initiatives' success poses CSRM challenges due to the difficulties of implementing risk management processes and cultures (Oliveira et al. 2019) and all basic cybersecurity practices (Maurer et al. 2021). Issues of ineffective practices, possibly through unawareness of success factors for CSRM implementation (Zammani and Razali 2016) and potential vast negative direct and indirect impacts perpetually rocking the foundations of businesses embracing the gains of internet revolutions unto foreseeable future (Singh et al. 2018). Some organisations become more successful at identifying, detecting and responding to these CSRM threats and risks in the quickest time frame than the Small and Medium Enterprises (SMEs) with notable weak characteristics and passive risk management systems (Kabanda, Tanner and Kent 2018; Yaraghi and Langhe 2011).

A large body of empirical studies focused on cybersecurity issues and challenges flourish in Nigeria due to ICT advancement (Lamidi 2020; Makeri 2017). Limited study explores cybersecurity strategies for preventing cyber exploitations in some financial industries using an integrated systems theory in a qualitative multiple case study (Alawonde 2020). Literature analyses success factors in a related field of CSRM (Usman 2013). However, there is limited literature on success factors that influence the success of CSRM in large organisations in Nigeria. Many authors perceived the importance of certain factors might impede the successful implementation of CSRM practices in organisations, including the high cost of risk management (Srinidhi, Yan and Tayi 2015), management support (Soomro, Shah and Ahmed 2016), geographic locations and cultural issues (Yaraghi and Langhe 2011).

Thus, further research is required to improve large organisations' practices, help stakeholders understand these factors and contribute to the CSRM implementation efforts and success. Though the literature documented models related to success factors for information security risk management, fraud prevention and cyber security frameworks, these models' validity and significance in CSRM implementation success in large organisations in Nigeria are under-researched. These proposed models supported the implementation process and practices in other countries, risk management areas and sectors but not in large organisations in Nigeria. CSRM implementation practices and approaches differ in matching organisational complexities (Schiller and Prpich 2014).

There are diverse opinions that the factors that influence CSRM implementation success differ among countries and organisations depending on national/political culture, organisational type, and size (Chang and Ho 2006; Werlinger, Hawkey and Beznosov 2009). For instance, the literature indicates differences in success factors in the practice of CSRM in large organisations and unprepared SMEs (Aladenusi 2021). Moreover, influential factors vary in financial, healthcare and e-retail organisations. Although some factors are common in these models, no specific model investigates success factors for CSRM implementation in large organisations in Nigeria. Furthermore, private organisations' management styles, decision-making, CSRM and implementation processes differ significantly in Nigeria's government organisations.

Investigating literature brings to fore the issues mentioned above and many questions regarding the factors influencing successful CSRM implementation within this chapter. Chapter one introduces the research scope and provides the study's context discussed in detail in subsequent chapters. Section 1.2 describes the background of the study, while section 1.3 explains the thesis problem statement. The research rationale and gap, aims and objectives are defined, research questions are formulated in sections 1.4, 1.5 and 1.6, respectively. The thesis structure is presented for the smooth flow of argument and easy readability in section 1.7. Finally, it concludes in section 1.8.

1.2 Research Context: Cybersecurity Risk Management in Large Organisations

Cyber security risk management is a critical strategic concern in organisational management (Rothrock, Kaplan and Van Der Oord 2018). The advanced expansion of the internet and information technology necessitated the explosion in business growth (Aminu 2013; Kikwasi 2018). Implementing effective CSRM is ever more gaining the attention of academics and

practitioners (Kahyaoglu and Caliyurt 2018; Islam, Farah and Stafford 2018). While information is essential and critical for information and communication technology organisations, the dark side has evolved and inflicted coveted worldwide targets. Therefore, the widespread venom of cyber security threats and risks becomes a puzzle for unravelling organisations.

Cyber security has not just become a buzzword used in recent decades, but a multi-dimensional growing problem that can have a significant impact, requiring elaborate mitigation activities inevitable for business survival. A few academic published papers have clearly defined the concept of cyber security despite its strategic importance to organisational success (Chen and Duvall 2014).

Cyber security risks and threats turn ‘the good’ advantages of technological innovations and business growths to ‘the bad’ and ‘the bad’, ‘the ugly’ (Kim et al. 2011). Developing countries are much more disadvantaged than developed countries in the business domain (Frank and Odunayo 2013). In Nigeria, fondly called “the Giant of West Africa” by size and economy (Falola, Genova and Heaton 2018), above 80 per cent of E-retails are ripe targets for cyberattacks for obvious reasons, including poor internet infrastructure, cultural barriers, inadequate regulatory framework, security issues and much more (Aminu 2013). Nigeria experiences more security infringements, cybercrime and fraud issues (Abdul-Rasheed et al. 2016); 86% of Nigerian companies fell prey and ranked 47th in Global Cybersecurity Index (ITU 2022).

Managing cybersecurity risks and threats in cyberspace are interwoven and inherently challenging for organisations to establish a comprehensive, problem-solving risk management system that captures and clarifies the scope and the complexity of interaction between the two worlds. The successful implementation of an effective response to the explosion of increasing diversity and sophistication of cyber threats requires a broad range of technical, financial and human resources within very few countries (Kumar et al. 2020; Tagarev 2020).

Similarly, Chief Information Security Officers' (CISOs) responses to cyberattacks among retailers in the UK indicated that the average cyberattacks increased to approximately 400-500% more than the previous year (BRC 2020). Over 4,800 unique retailers' websites globally compromised customers’ credit card details monthly (Symantec 2019). More critical cybersecurity-related issues with multiple challenges are associated with managing these risks (Shackelford 2016). Agile and timely management of the threats and vulnerabilities frighten top management business managers, customers, and investors of businesses of all sizes.

Few organisations have mature risk management processes and harness their significant strategic value (Beasley et al. 2020) to reduce the uncertainty of achieving their objectives. Therefore, risk management has become necessary for businesses to ensure operational success, organisational stability, win customers' trust and be a helpful governance tool for policymakers (Saunders 2017). Performing risk management in a cyber-security context continuously calls for a search and demand for a robust CSRM inspired by a holistic view of its appropriateness and effectiveness. Therefore, this research will understand cybersecurity risk management as

> *"a continuous decision-making process to identify and prioritise critical components such as organisational, human and technical factors and risk management practices by implementing and monitoring controls, efficiency and operations' effectiveness to achieve the organisational goals".*

1.3 Problem Statement

The problem is that despite the cybersecurity risk management solutions to mitigate cybersecurity challenges, the rhetoric and the losses of cybersecurity incidents exacerbated by the pandemic are on the increase, and organisations are still unable to manage these problems effectively (Ajah and Chukwuemeka 2019; Dalal et al. 2021; Wang, Nnaji and Jung 2020). These problems include the elaborate mitigation activities and the faulty implementation practices of cybersecurity measures (Okolo 2016, Oforji, Udensi and Ibegbu 2017); limited knowledge of asset identification (human, technical); minimal valuation and loss estimation (most unreported attacks and losses); the business case to invest adequately (Fenz et al. 2014); failure to efficiently manage critical security/information assets (Von Solms and Van Niekerk 2013); culminating in social, technical and legal factors that challenge CSRM implementation.

These challenges include complexities of technical factors such as lack of appropriate technologies and infrastructures leading to cyber-attacks, legal challenge of fragmented regulations, operational/social challenge of lack of expertise and skills gap. Undoubtedly, the pandemic exacerbated cybersecurity risks and challenges of secure access with rising mandated work from home opportunities for many corporate organisations.

The technology giant (Google) reported over 46,000 new phishing websites weekly globally (Transparency report 2020). A staggering 2.3 billion breached data records worldwide (Irwin 2021). Limited studies focused on the sociological and technological factors that influence

cybercrime that impacts Nigeria's cybersecurity (Olayemi 2014). This study does not seem to offer any accepted solution for these problems but primarily marginalised to mainstream national failures of the security agencies and weak cybersecurity laws.

Failure to secure and manage company's critical assets such as information, technology, people, process and the conflicts between business and security objectives, through the implementation of essential controls efficiently threatens not only its existence but also jeopardises its competitive advantage (Von Solms and Van Niekerk 2013; Atoum, Otoom and Abu Ali 2014). The traditional tendency to manage cybersecurity risks from a technological perspective and within the information security system entity may not be sufficient (McEvoy and Kowalski 2019; Öğüt, Raghunathan and Menon 2011).

Cyber Security Risk Management is an ecosystem; its components are interconnected and integrated, necessitating qualitative, subjective knowledge and risk management implementations to succeed (Tisdale 2016). Experts continue to call on organisations to be more strategic towards managing cybersecurity risks and these assets (technology, people, process (Atoum, Otoom and Abu 2014, Soomro, Shah and Ahmed 2016) as cybersecurity and online security of businesses become more important than ever (BRC 2020). In sharp contrast, it has not been clear what such an approach looks like in practice or how firms achieve this (Diesch, Pfaff and Krcmar 2020).

Organisations that consider cybersecurity technical and non-technical aspects are typically more successful in securing their security/information assets (Ifinedo 2012) and optimising the socio-technical management process cybersecurity practices (Malatji, Marnewick and von Solms 2020). Organisations and academics struggle to find an effective solution that encompasses technical cybersecurity and improves people and processes. There has been no conclusion due to the highly secretive nature of the topic. It does not lend itself to a simple investigation, very intrusive and reasonably comprehensive, requiring a cautious approach with good rapport.

Moreover, in the empirical cybersecurity research, success factors for CSRM implementation are a neglected area, under-looked. These problems mentioned above means: (a) the concept of CSRM is still evolutionary, (b) the need for the design and implementation of effective coordination and balancing of cybersecurity and business need, (c) the appropriate address of the exploitation of the vulnerabilities and the challenges that can arise from multi-faceted CSRM work activities, processes, resources, and capabilities within the organisation and manage various stakeholders at multiple levels, (d) for the dynamic business processes to match the pace of

technological advancement, the overall strategy needs to be iterative, use appropriate and efficient methods and at the same time be cost-effective (Cîrnu et al. 2018).

Examining cybersecurity literature brings various questions regarding the factors that contribute to the successful implementation of CSRM that were not fully covered in prior studies but needed more significant attention. Do we continue to live with the unintended consequences of digital transformation? Why do businesses still struggle to achieve adequate cybersecurity? How can large companies in Nigeria succeed in implementing CSRM in their operations amid all these security challenges to achieve their goals?

Thus, this research addresses these problems by exploring a socio-technical framework with a success factors model to help organise and improve managing cybersecurity risks and practical response to control implementation problems and desired positive outcomes in large organisations and businesses in Nigeria from theoretical and empirical perspectives as case studies and benefit both future researchers and practitioners.

1.4 Research Rationale and Gap

Nigeria, the 8th largest worldwide internet user, have a strong predominance of highly digital, banked mobile consumers, particularly in e-commerce, banking and telecommunications (Olasanmi 2019; Wang, Nnaji and Jung 2020). Cybersecurity issues and CSRM in Nigeria are challenging and of great concern worldwide, mainly because attackers are becoming more innovative in their fraudulent gainful employment (Wang, Nnaji and Jung 2020).

The evolutions of Nigerian ‘kings of malware’ in scope, size, technical competence and intricacies facilitate complex networks to successfully attack their profitable coveted targets (businesses, large organisations and governments) for globally lucrative returns from organisations (Hinchliffe 2017). The business scope and consumer processes where technology facilitates intensive business activities became vulnerable (Goni 2019) and gave rise to the unique attendant profile of rea and varied categories of cybercrime threats and risks. Phishing, bot attacks, leaked customer data and breaches (identity frauds and thefts) are described as perfect storms unfolding by day (Aminu 2013; Ulsch 2014).

Many studies focused on Nigeria's cyber security issues and challenges (Frank and Odunayo 2013; Oforji, Udensi and Ibegbu 2017). Few researchers have singly addressed some management

problems (Okolo 2016; Osho 2015). Some studies have investigated management's role in combating cybercrime and success factors for preventing e-banking fraud in the Nigerian banking industry (Ogoh 2016; Usman and Shah 2013). Cybersecurity is projected to be the top news headline (Aladenusi 2020), with more malicious phishing schemes taking advantage of economic, social, and political conditions worldwide (Aladenusi 2021).

Cyber security and risk management are increasingly becoming concerns and a remarkable feature in information systems, technologically and managing organisations operating online (Chen and Duvall 2014; Meszaros and Buchalcevova 2017). The notion of efficient CSRM, a central issue, has gained attention in the last decade (Vakharia, Mishra and Kumar 2012). Research interest in organisational management and sustainability increases (Akinwumi et al. 2017; Chabinsky 2014; Musman and Turner 2018).

Many organisations are still experiencing cybersecurity issues irrespective of the efforts- risks, threats, vulnerabilities and incidents (Dalal et al. 2021). Organisations usually commit to CSRM initiatives, unaware of the keysatisfy factors contributing to their implementation success (Zammani and Razali 2016). A review of published studies on risk management reveals that success factors for implementing risk management systems in developing countries continued as an under-researched area of study (Reza Hosseini et al. 2016).

The exclusion of studies in the socio-technical success factors to CSRM implementation in Nigerian organisations further establishes a gap in prior studies. Top management is under immense pressure to make sound cybersecurity decisions and investment choices within an enterprise-wide focused risk management programme. Such an economical set of control measures (people, technology, and process) can be selected to continuously identify, prioritise, document, and mitigate cybersecurity risks to an acceptable level (Matthews, Arata and Hale 2016; Mazzoccoli and Naldi 2020). Little is known about how organisations protect themselves in practice (Baskerville et al. 2018).

An emerging quantitative study of the current state-of-the-art cybersecurity breaches, practices and capability of the Nigerian internet banking industry revealed limited published literature in this area (Wang, Nnaji and Jung 2020). The study suggests a holistic approach to the Nigerian banking industry's key challenges with more face-face qualitative studies for more reliable results in recent cybersecurity research (Fujs, Mihelič and Vrhovec 2019). Current cyber security risk

assessment methods attempt to address CS issues' challenges and propose a risk-based decision framework for prioritising cyber security strategy (Ganin et al. 2020).

The socio-technical cyber security systems applications to risk management have been recommended as a holistic business function in enterprise system security (Malidjit et al. 2020). There are common opinions that a comprehensive approach to CSRM is complicated and costly. Very few organisations, including large environments, can successfully implement CSRM (see section 4.5.3). There are differences among influential factors in financial (Camillo 2017; Dugg 2015; Power, Ashby and Palermo 2013), SMEs (Kabanda, Tanner and Kent 2018) and other organisations.

There are models of success factors in related fields of CSRM implementation, such as information security risk management (Safa, Von Solms and Furnell 2016; Webb et al. 2014) fraud prevention (Usman and Shah 2013). Likewise, the literature has reported cybersecurity frameworks (Gourisetti, Mylrea and Patangia 2020; Masike, Sune Von and Marnewick 2019). However, there is little agreement on these models' applicability and validity since they are not generic and have not yet established whether they are applicable in CSRM implementation success in large organisations in Nigeria.

It is often impracticable to transfer and apply the same CSRM factors and implementation practices across organisations due to differences in organisational type, decision-making processes and unique attendant risks. In the light of recent events in CSRM, the growing common theme in Nigerian cyber security domain reports and research revolve around the intractable challenges of cyber security among individual internet users, banks, and the nation. Moreover, these studies focus mainly on the banking industry without the other non-financial sectors.

The critical literature analysis across various regions shows that these factors are reasonably comprehensive. Sadly, certain aspects that appear relevant and better localised to the Nigerian context seem to be completely absent or scarcely implied. Such includes understanding the current CSRM implementation state, practices, development, and advancement to address the implementation issues in cyber security warfare adequately.

Despite these interests, the specific areas of holistic studies on factors that influence CSRM implementation success in Nigeria have been neglected to the best of the researcher’s knowledge. This research represents one of the few. Against this backdrop, this research chooses to extend

the frontiers of knowledge by filling these gaps. The background discussion leads to the crucial unaddressed research problem (success factors for CSRM implementation) that needs evolving emphasis on more empirical and in-depth research. Therefore, large organisations (the coveted prime targets of cybercriminals) need to harness progress support towards awareness and the importance of socio-technical factors that influence the success of CSRM implementation and harmonise them to yield the desired outcome.

Hence, CSRM implementation success in Nigeria is of utmost priority for organisations' survival, public trust, and national and worldwide cyber peace. What factors influence the success of implementing CSRM? According to the paradox, 'we do not know what we do not know'. A comprehensive and balanced system of exploration of CSRM implementation needs to be developed and studied empirically. Moreover, there is a need to understand why specific organisations implement CSRM successfully, while at the same time, others struggle to do so (Choobineh et al. 2007). This problem merits investigation. Hence, this research contributes to previous CSRM literature to bridge and fill the gap in CSRM implementation in large organisations in Nigeria by optimising the socio-technical factors for CSRM implementation success. The study started with a single aim which guided and served as the focus for this research.

1.5 Research Aim and Objectives

Little research has been done to understand those factors contributing to CSRM implementation success at the organisational level in Nigeria (Oforji, Udensi and Ibegbu 2017; Osho 2015). The background discussion and analysis of success factors influencing CSRM (chapter 2) reveal the research rationale and gap discussed in section 1.4. In collaboration with the problem statement, these sections confirm that CSRM is a growing problem with increasing risks such as financial risks, operational risks, reputational damage, and much more.

Thus, there is a need to help organisations in Nigeria take vivid advancement to understand the factors that influence CSRM implementation success. Literature reports that the socio and technical factors and business processes must be considered for optimal CSRM practices (Malatji, Marnewick and von Solms 2020; Masike, Sune Von and Marnewick 2019; Sarker et al. 2019). Thus, the thesis aims to:

> *"Explore success factors influencing the implementation of CSRM in large organisations in Nigeria".*

This study highlights the *need* for a success factors model for CSRM implementation. Although the analysis of some factors (for example, management support, awareness, and training) in the literature necessitate understanding, evaluating, and explaining them in large organisations. The large Nigerian organisations can transform the conceptual framework of success factors into a model that supports their decision-making process for CSRM implementation efforts and practices. This study attempts to enhance these by: (a) identifying various factors for CSRM implementation success, (b) evaluating which factor(s) may influence CSRM implementation success (c) prioritising the importance of success factors for CSRM implementation. The model will guide large organisations' management and stakeholders to make the right decisions to enhance successful CSRM implementation practices.

Below is the outline of the objectives to address the research aim:

- Objective 1: To critically review the success factors in CSRM literature and understand the area focusing on large organisations.
- Objective 2: To identify and evaluate factors influencing CSRM implementation success in large organisations in Nigeria.
- Objective 3: To develop and propose a model of success factors of CSRM implementation in large organisations.
- Objective 4: To validate and evaluate the model within the practical arena and develop a novel contribution to the domain of large organisations and CSRM implementation.

1.6 Research Questions

The background discussions show that most organisations in Nigeria are vulnerable to CS risks and threats. The primary research question identified to achieve the research objective is:

- *What success factors impact CSRM implementation in large organisations in Nigeria?*

The following questions could further capture the aim, investigate, and answer the research question in more detail. These research questions form the basis for the theoretical framework for the empirical study from the socio-technical perspective:

- What are the People factors associated with CSRM implementation success in large organisations in Nigeria?

- What are the Technological factors associated with CSRM implementation success in large organisations in Nigeria?
- What are the Process factors associated with CSRM implementation success in large organisations in Nigeria?
- What are the Organisational factors associated with CSRM implementation success in large organisations in Nigeria?

1.7 Thesis Outline

.

The thesis outline takes the form defined by Phillips and Pugh (2010), comprising four elements: background theory, focal theory, data theory and novel contribution. Background theory demonstrates having professional knowledge of the field of study (Chapter 1), evaluating contributions in research, and identifying areas of theoretical and empirical weakness (Chapter 2). The focal theory establishes the problem's nature and generates a conceptual model (Chapter 3). The third element (Data theory) contents discussed in Chapter 4 of the thesis include (a) engagement and justification for the epistemological position, (b) the advancement of the methodological research choice and (c) the suitability of the chosen research strategy. Furthermore, the justification for collecting and analysing data discussed in Chapters 5 and 6 form part of the data theory element. The final aspect (new contribution) outlines and evaluates the study's relevance for advancing the researched domain (Chapters 7). Chapter 8 summarises the research discussed in this thesis highlights further studies' suggestions and recommendations. This thesis outline is organised into eight chapters, each providing the analytical constructs viewed as relevant to this research. Figure 1.1 illustrates the thesis outline and discusses it in the subsequent sections.

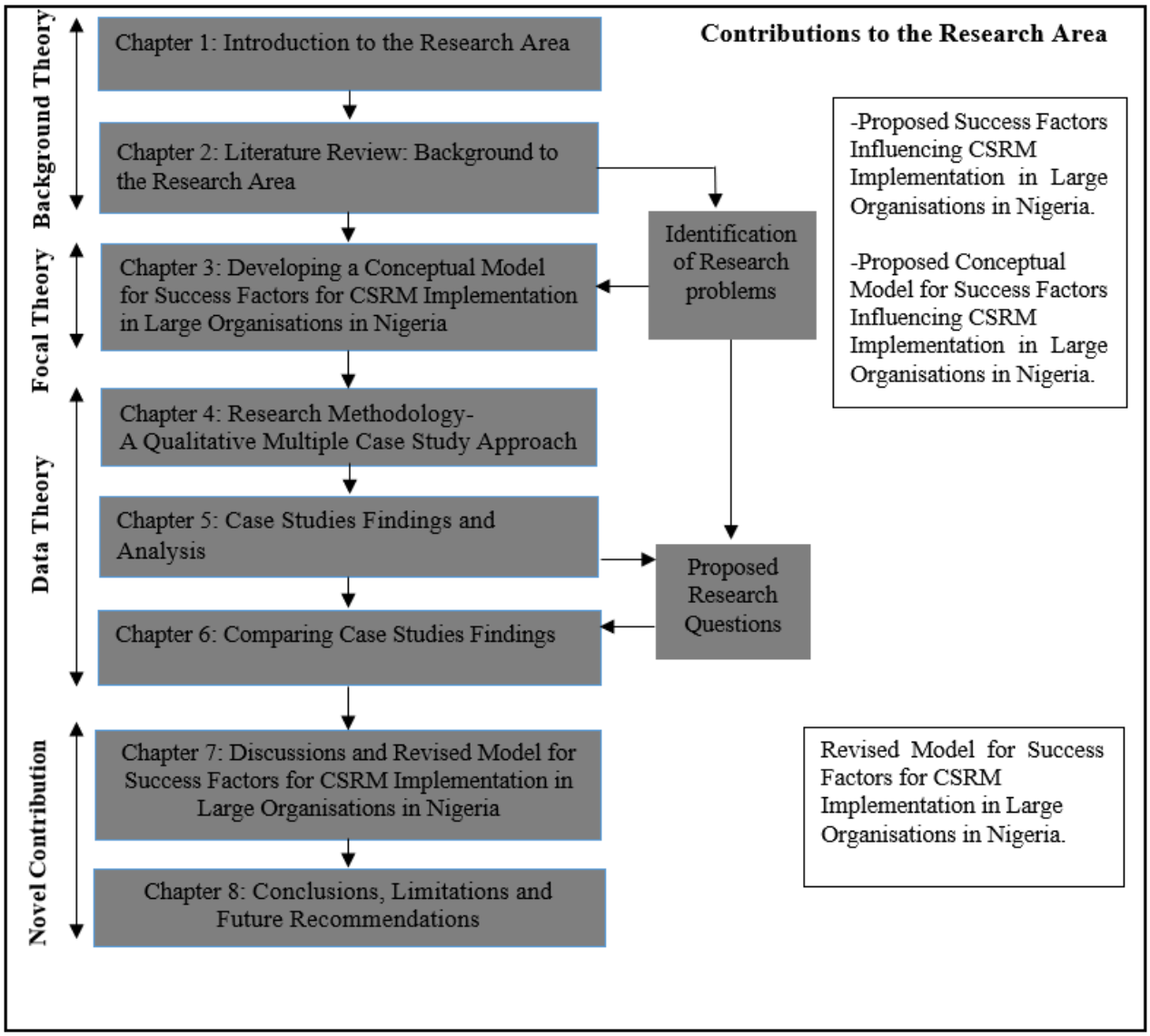

Figure 1.1: Thesis Outline

1.7.1 Chapter 1: Introduction to the Research Area

Chapter 1 introduces the central problem addressed in this research by focusing on success factors and large organisations. The issue under study focuses on identifying and evaluating the factors for effectively managing this problem and improving CSRM implementation success in large organisations in Nigeria. Next, the aim, objectives and research questions are presented with the thesis outline (Figure 1.1).

1.7.2 Chapter 2: Literature Review

The brief introduction to the research field and scope now established in chapter two begins by creating the criteria to demonstrate the worth of the literature review (Table 2.1). Following that, qualitatively reviews existing literature on CSRM. Initially, it discusses some definitions of cyber security and taxonomies of cyber security risks and threats. Further, it discusses some Risk definitions (Table 2.2) and Risk Management definitions (Table 2.3). Based on prior cyber security and Risk Management definitions and identified attributes of the cyber security domain and the risk management process, a succinct explanation for CSRM was provided and further discussions on the relevance of CSRM to large business organisations. Next, critically reviews prior literature on success factors for CSRM and in related disciplines and large organisations. Then establish the scope on success factors for CSRM area by discussing the socio and technical perspectives: (a) the current research on Organisational Factors (b) the present research People Factors (c) current research conducted on Technology Factors and (d) current research conducted on Process Factors in large organisations. Finally, it highlights the literature's research objectives for further investigation with several justifications (Section 2.8).

1.7.3 Chapter 3: Developing and Proposing a Conceptual Model

Applying a socio-technical approach, Chapter 3 introduces and proposes a conceptual model for success factors influencing CSRM implementation in large organisations in Nigeria (Figure 3.1). The framework is underpinned by the Socio-technical theory and the Information Systems Success Model. The proposed model can be helpful as a decision-making tool and assist management while making important CSRM implementation decisions. Researchers and practitioners can also use the model as a guideline to improve CSRM implementation practices in large organisations in Nigeria.

1.7.4 Chapter 4: Research Methodology–A Qualitative Multiple Case Study Approach

Chapter 2 sets the research background, while Chapter 3 suggests the conceptual model for success factors for CSRM implementation in large organisations in Nigeria. These chapters helped understand and identify research problems for more investigation. A research methodology is applied to verify the proposed conceptual model in practice organisations to examine the research problems. Chapter 4 states the justifications for the choice of a specific

research methodology. Then reviews different research philosophies, says their inherent inadequacies, and provides the suitability to this research.

1.7.5 Chapter 5: Case Studies Findings and Analysis

Having understood all the relevant research problems, the thesis then describes the case studies conducted in four large organisations in Nigeria and empirical data analysis. Chapter 5 begins with the pilot case studies and presents the background to these large organisations. Further, it explains and analyses the main problems, including (a) pilot case studies, (b) discusses data coding of the semi-structured interviews with 30 participants and analyses the factors influencing CSRM implementation success via thematic analysis using NVivo 12. The data collected results provide significant findings and discussion of the background to the case studies and assess the research questions.

1.7.6 Chapter 6: Comparing Case Studies and Discussions

The four case studies' comparative analysis examines those success factors within the four case studies influential in the successful implementation of CSRM, as earlier discussed in Chapter 5. It provided in-depth knowledge and a clear understanding of how these success factors enhance successful CSRM implementation in large organisations in Nigeria.

1.7.7 Chapter 7: Revised Model

Based on the case studies and research findings from the empirical analysis in the previous chapter, the current chapter briefly highlights the present research, reports the thematic analysis results, explains the lessons learnt from the case organisations and (a) revises the existing factors influencing the success factors for CSRM in the case organisations, (b) describes the new factors discovered through the empirical findings, (c) the results are then discussed with present findings from prior related studies, (d) updates literature with revised factors influencing CSRM implementation success in large organisations in Nigeria and describes the new CSRM implementation success factors. As a result, they are satisfying the aim of this thesis by proposing a revised model for CSRM implementation success in large organisations in Nigeria to decision-makers and researchers.

1.7.8 Chapter 8: Conclusions, Limitations and Future Recommendations

Chapter 8 presents this thesis research overview. The research findings discuss the thesis by considering the study outcomes concerning the research questions, aim and objectives. Subsequently, it discusses the unique research contributions to knowledge and implications for practice. Lastly, it highlights the necessary conclusions for the chapter and this thesis, the study's possible limitations and suggestions for further research.

1.8 Conclusion

The research accomplished within this chapter concludes that CSRM is a part of doing business but must be managed well in a risk management process. Undoubtedly, CSRM is a hot topic in all industries, especially largerealisation organisations worldwide. Although cyber security risks and attacks may seem inevitable, achieving the desired CSRM implementation success is practically demanding. However, wrongly implemented CSRM practices without a thorough understanding of its success factors will consistently be a challenge and a false security net to such organisations.

Consequently, socio-technical factors in CSRM implementation success call for bravery and immersion by all stakeholders in a large organisation in Nigeria. Cyber security risk management is an emerging research area in Nigeria; thus, there is a lack of theoretical and conceptual models highlighting the factors that influence its implementation success in organisations in Nigeria. This shows that identifying and evaluating factors that influence CSRM implementation in large organisations in Nigeria is imminent. Furthermore, to address this theoretical gap, this study attempts to extend the socio-technical theory to CSRM and develop a CSRM implementation success factor model to improve its CSRM implementation process and practices. The value of implementing a comprehensive CSRM socio-technical success factors model is paramount to map the organisation to the balance between detection, prevention, and response to any situation.

Chapter 2: Literature Review

2.1 Introduction

This study discovered that very little is known about factors influencing CSRM implementation success in large organisations. Findings from existing studies of CSRM in related fields, other sectors and countries may explain the subject of CSRM. Nevertheless, they cannot be generalised or applied to large organisations in Nigeria without validation. One possible explanation among others is due to the significant difference among the sectors in large part due to the peculiar attributes of large organisations in Nigeria such as (a) Economic climate, (b) operational and functional activities, (c) governance structures (d) business culture with goals (e) ease of access to information and communication (f) decision-making process (g) management styles.

The literature review transcends previous research precis with a list of success factors influencing CSRM implementation in large Nigerian organisations. It is a rigorous summary of critical analysis of selected, relevant published and unpublished literature read and references focusing on the topic under study (Hart 2018). Chapter 2 reviews prior studies their methodologies and discusses the critiques in literature. The chapter starts by establishing the criteria for the literature review (Section 2.2). The second section explains cybersecurity (Section 2.3) and the Risk Management theme by giving an overview of Risk and Risk Management (Section 2.4). Next, it conceptualises CSRM (Section 2.5) and explains the link between CSRM and the existing risk management frameworks (Subsections 2.5.1).

Section 2.6 commences the review of prior works of success factors influencing CSRM implementation. Section 2.7 critically analyses CSRM literature and related CSRM literature identifies, explains, and prioritise the success factors for CSRM from socio-technical perspectives within the private and public domain, including different geographic locations. The critiques of literature reviews of the factors for the successful implementation of the CSRM defined and evaluated the needed contribution of the study (Section 2.8). The section highlights the research gap and concludes with investigating the success factors for CSRM in large organisations in Nigeria (Section 2.9). Further, to adopt a suitable theory that underpins the research to create a model that offers a detailed view of the factors helpful in identifying and validating success factors that influence CSRM implementation in Nigeria later in Chapter 3 of this thesis.

2.2 Criteria for the Literature Review

The important feature in all research is the literature review. Literature reviews generally provide an overview, synthesis, and critical engagement with previous research, identifying a problem or challenging existing knowledge and formulating new or likely research questions that lead to more prominent theories (Alvesson and Sandberg 2011). Table 2.1 illustrates the criteria for the literature review practice, which form the basis for this study.

Table 2.1: Criteria for the Literature Review (*Source: Boell and Cecez-Kecmanovic 2015*)

This item has been removed due to 3rd Party Copyright. The unabridged version of the thesis can be found in the Lanchester Library, Coventry University.

2.3 Cyber Security

Cyber Security (CS) has emerged as a widely used term with increased adoption by practitioners. Extant literature identifies the main definitions and interpretations of authoritative sources for the word 'Cyber Security. Cyber Security and information security are often used synonymously with no difference (Öğüt, Raghunathan and Menon 2011). However, CS and information security are not entirely similar concepts but overlap (Von Solms and Van Niekerk 2013). To understand the two words' opinions, it is essential to investigate their underlying ideas.

Information security is protecting the confidentiality, integrity, and availability of information assets, whether in storage, processing, or transmission, via policy, education, training, awareness, and technology (Whitman and Mattord 2011). This definition shows information as an asset to be secured with its characteristic features, namely Confidentiality, Integrity and Availability (CIA triad) (Von Solms and Van Niekerk 2013). Availability implies that authorised individuals should

only access the information correctly represented (Integrity) without disclosure (Confidentiality) to unauthorised individuals.

Some definitions of information security narrowly focus on the CIA Triad; authentication and non-repudiation should be incorporated into the 'CIA Triad' as a 'security star' (Raggad 2010). Authentication means the system or human identity verification before granting access permission, while non-repudiation is a mechanism intended to fulfil standard requirements. These five elements constitute the security goals that contribute to achieving the organisational objectives (Raggad 2010). There is no doubt that these attributes and perspectives are remarkable and should be pursued, but certain CS truths seem evident. Cyber Security has diverse phases of evolution; the first phase, the security of the CIA purely technical in nature, while the second phase involves the security of the human element (Veiga and Eloff 2007) and many more unfolding (McShane, Eling and Nguyen 2021). The acclaimed Triad, non-repudiation and authenticity goals are not the end product of the CS implementation programme and should not be seen in like manner (Goss 2017).

Cyber Security is defined as 'the protection of cyberspace itself, the electronic information, the ICTs that support cyberspace and the users of cyberspace in their personal, societal and national capacity, including any of their interests, either tangible or intangible, that are vulnerable to attacks originating in the cyberspace' (Von Solms and Van Niekerk 2013). Consider, for example, Mitnick and Simon (2011), fully endorsed by experience, maintains that security is a process. This means CS encompasses processes, technologies and controls designed to protect systems, networks and data from cyber-attacks and humans that work on these processes, technologies, and controls. The definition shows that CS is part of information security, Information and Communication Technology (ICT) security and everyone (individuals, nations, or organisations) functioning in the vulnerable cyberspace. Von explains that the asset to be secured in ICT is the underlying technology; the asset (s) to be secured in information security is the information and the resulting threats and vulnerabilities of its underlying technologies.

On this premise that CS links with information security, CS is protecting the CIA of digital information assets vulnerable through the internet against threats (von Solms and von Solms 2018). Von clearly explains that the internet represents the main domain where CS takes place for the protection of confidentiality, integrity and availability of vulnerable information assets against any security attacks or threats. This means that determining the best course of action for the protection and monitoring controls to protect everything or anything, whether data or

information, technology, or storage sources from unauthorised electronic access (i.e., cyber realm), plays a significant role in CS. Figure 2.1 shows the relationship between the three.

This item has been removed due to 3rd Party Copyright. The unabridged version of the thesis can be found in the Lanchester Library, Coventry University.

Figure 2.1: Relationship between Information Security and Cyber Security

(Source:Von Solms and Van Niekerk 2013:101)

A closer look at Figure 2.1 above shows that CS involves vulnerable things through ICT, digital and non-digital information, and non-information-based assets such as devices and technologies associated with the cyber realm. On the other hand, information security protects both analogue and digital forms of information regardless of the domain. From the above, one can conclude that CS is an umbrella concept that incorporates information security and ICT security.

The ITU (2008:2) defined CS as 'the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can protect the cyber environment, organisation and user's assets.' This definition relates to an operational aspect of CS. These definitions above show a broad range of security elements, emphasising both technical and non-technical assets to be protected. These assets include any valuable thing in the organisation, including information, servers, laptops, people, databases, and buildings.

Information security and Cybersecurity have security components in common: confidentiality, integrity, and accountability (Jung 2011). The difference is that CS can address other dimensions not addressed by information security (Safa, Von Solms and Furnell 2016). The growing nature of cyberspace and the paradigm shift of managing the human elements in the domain allows CS to have unique traits such as socio-technical, socio-organisational, socio-legal, and socio-cultural dimensions not addressed by information security (Mitnick and Simon 2011; Von Solms and Van Niekerk 2013).

The connectedness in CS clearly distinguishes it from information security. This study aligns with the comprehensive empirical research of the term CS as 'The collection of tools, policies, security concepts, security safeguards, guidelines, risk availability of data and assets used in cyberspace. The concept includes guidelines, processes, policies and collections of safeguards, technologies, tools, and training to provide the best protection for the state of the cyber environment and its users' (Schatz, Bashroush and Wall 2017:64).

Cyber Security, therefore, is not information security dedicated to perimeter fencing around information technology, but a business issue involving the protection of everyone and everything that functions in cyberspace (Von Solms and Van Niekerk 2013; Rothrock, Kaplan and Van Der Oord 2018). Therefore, within a CS programme, an organisation must first understand and define its risk(s) to manage it effectively (Hagigi and Sivakumar 2009; McEvoy and Kowalski 2019). However, in the security domain, many risk definitions exist. The following section discusses some terms to understand the concept of CSRM effectively.

2.4 Risk and Risk Management

Cyber-attacks have brought risks to more limelight (Hopkins 2017). Whether big or small, organisations are always at the 'risk' of CS from faceless enemies; risk management is a dynamic industry with imagination's fecundity. A thorough understanding of risk definitions leads to a wealth of knowledge and better competence to manage it (Andersen, Garvey and Roggi 2014) before presenting and discussing risk management.

2.4.1 Risk Definitions

Authors and researchers from various professions have different definitions for risk based on their

circumstances and adopt concepts and terminologies that suit them (Dionne 2013; Haimes 2009; Touhill and Touhill 2014), as highlighted below (Table 2.2).

Table 2.2: Risk Definitions

Definition of Risk	References
A measure of the probability and severity of adverse effects	Haimes (2009)
Effect of uncertainty on objectives	ISO/IEC (2016)
The function of the interaction of threats, vulnerabilities, and likelihood (or probability) of threats acting against a business	Touhill and Touhill (2014)
An uncertain event that could positively or negatively affect the achievement of objectives subject to its occurrence	Best Management Practice (2009)
Combination of probability and consequences	Ben (2009)

From the above, risk is defined in terms of the likelihood and impact of adverse effects (Haimes 2009). Ben (2009) considers risk in terms of its impact on organisational objectives. The functional perspective (Touhill and Touhill 2014) and the management view defined risk as planning, organising, controlling, and directing to prevent threats and attacks that affect an organisational objective (Best management practice 2009). ISO/IEC (2016) defined risk as the effect of uncertainty on achieving corporate objectives. Knight defines uncertainty as an action or incident that could occur in the future without control (Toma, Chiriţă, and Şarpe 2012). No one has an accurate prediction or estimate of the chance of a CS incident happening or the extent of the damaging effects in any organisation.

The above shows that uncertainty links with the organisational objectives, and an organisation exist to achieve its stated goals. This study agrees with ISO/IEC (2016) in its definition of risks as preventing and mitigating uncertain cyber risks and events, which are much more desirable than undergoing vulnerability remediation after a CS breach. Not knowing the risks is not the most significant risk to any business (Ryan et al. 2012), but a systematic way of controlling the risk (Ben 2009). Researchers and organisations begin to look for a way to manage CS risks in terms of risk management. Risk management practices continue to become more relevant in financial and non-financial organisations as a strategic management tool (Hull 2015).

2.4.2 Risk Management

The meaning and definition of risk management are not fixed. Risk management continuously evolves within many specialist disciplines that cannot avoid context, so one size does not fit all. Context is essential in risk management, likewise in this study, as shown in (Table 2.3) below.

Table 2.3: Risk Management Definitions

Definition	Risk factor	References
Coordinated activities to direct and control an organisation regarding risk	Organisation	ISO/IEC (2016)
Processes employed to protect IT assets from unauthorised access, misuse, manipulation, loss, modification, and inadvertent disclosure of data and information embedded in these assets.	Information assets, data, and the information contained in them	Kouns and Minoli (2011)
Information Technology Risk Management or Information Security Risk Management (ISRM)	Information Technology	Kouns and Minoli (2011)
Coordinate the application of resources to minimise unpredictable events' adverse impact on fulfilling organisational objectives and maximise opportunities.	Organisational objectives, resources (human, technology, funds)	Andersen, Garvey and Roggi (2014)
A process that is set to achieve the organisational objectives underpinned by a set of principles, supported by a structure/framework that raises the awareness to identify and treat threats and emerging risks in the process throughout the organisation by improving controls, efficiency, and effectiveness of operations.	Organisational objectives, process, and operations	Gjerdrum and Peter (2011)
The process that allows IT managers to balance the operational and economic costs of protective measures and achieve gains by protecting the IT systems and data that support their organisational missions.	Data and information technology systems	NIST-SP 800-30

Table 2.3 above shows the various definitions of risk management according to its purpose. Risks affect fulfilling organisational objectives, and many factors create uncertainties to achieve the set objectives (Gjerdrum and Peter 2011). Breaking down risk components (likelihood of occurrence of a threat, the vulnerability of systems and data) and reducing the impacts of the threat) inform how to efficiently address risk management in an organisation (NIST-SP 800-30). One can argue that only proper coordination of risk management maximises the opportunities of achieving the organisational objectives (Andersen, Garvey and Roggi 2014). This study chooses to define risk management as a collaborative process aimed at achieving the corporate objectives underpinned by a set of principles, supported by a structure/framework to evaluate and prevent emerging risks in the processes by improving controls efficiency and effectiveness of operations.

Risk management study assumes effective CS within an organisation could be achieved by analysing and understanding risks to make informed decisions about investments and develop requisite CSRM policies and controls (Collier et al. 2014; Talbot 2009). A risk management process incorporated into the organisational business culture must convert strategy into operational and achievable objectives (Yaraghi and Langhe 2011).

2.5 Cyber Security Risk Management

Cyber security and risk management definitions above show that CSRM involves applying the principles and process of risk management to the CS domain. Information Systems continue to evolve and interconnect businesses to increase access to information data, decentralise business processes, and flexibility to run businesses. Advanced security technologies are continually invented to mitigate technical vulnerabilities while human element exploitation increases (Mitnick and Simon 2011). The Global Data report from significant security companies shows that compromised passwords remain the highest cyber breach statistics (Sobers 2020). In contrast, phishing and Business Email Compromise (BEC) are prevalent and successful in Nigeria (Aladenusi 2020).

Spears and Barki (2010) defined security risk management as a continuous process of identifying and protecting information systems security risks by implementing and monitoring controls systems. The growing emphasis on risk management in CS emerged for several reasons: Firstly, as an enhanced strategy and methodology for information systems security (Hoffmann, Kiedrowicz and Stanik 2016; Webb et al. 2014). Secondly, risk identification, assessment and mitigation involve several human factors (Ani, He and Tiwari 2019; Hadlington 2017). Thirdly, organisations need to be more strategic in their approach to CS (Bissell 2013; Chen and Duvall 2014), although achieving this and what such a strategy looks like in practice is not too bright yet.

Uncertainties surrounding the CS environment could be understood, assessed, and managed effectively through the CSRM approach. The risk management process is essential for CSRM implementation success (Choo 2011; Meszaros and Buchalcevova 2017). A strategically focused CSRM strategy comprises technical solutions and the integration of social alignment with organisational objectives. These qualitative analyses and decisions form the ‘Achilles' heel’ for an organisation (Tisdale 2016).

Tisdale (2016) found some characteristics of CSRM in an organisation, including risk as a business risk whose priorities must be determined by the senior leaders. Most threats originate from the insiders, and CS must involve managing human personalities. Also, organisations must position themselves with resources for immediate detection, treatment and recovery from complex and ever-changing threats and malicious activities. Modelling human behaviours and attack vectors increase situational awareness, informed decision, and acquisition processes. Furthermore, organisations should create an enabling CS environment using psychological and

anthropological techniques to identify and manage prospective offenders. There is a need for organisations to understand and enforce the law when needed. Finally, the possibility of the Risk Management Framework becoming a compliance checklist.

Based on the above discussions, designing and implementing successful CSRM in an organisation demands new thinking toward applying risk management at two key strategic levels: First, the technical level where key assets are the information technology services. This involves analysing CS (cyber activities) threats resulting from information security breaches (CIA breaches) with a high impact on cyber business. Understanding threats is key to identifying risks and vulnerabilities (Tisdale 2016). Therefore, understanding the interrelationships between these threats and business processes is essential for CS success. Second is the socio-technical level, where the main assets are cyber and security activities. These include the analyses of risks associated with CS breaches (CS risks) to determine the acceptable risk tolerance levels. It is pertinent to note that risk identification and assessment can only be sufficient when people at the level have adequate knowledge of cyber activities and their businesses' security. This makes the process less quantitative than qualitative.

Designing and implementing CSRM preventive and mitigative measures requires cooperation, balance, and alignment between the two levels discussed above to achieve success. This suggests the road to accomplish acceptable CSRM levels. The importance of CSRM is also evident by the issuance of a new framework for CSRM by the Central Bank of Nigeria to help businesses meet the growing challenge (CBN 2018). Risk management is part of an organisation construct that includes governance and policies (McFadzean, Ezingeard and Birchall 2006). However, studies have been scarce on implementing risk management in cyber security.

Thus, this study conceptualises CSRM as “a continuous decision-making process to identify and prioritise critical components such as organisational, human and technical factors and risk management practices by implementing and monitoring controls, efficiency and operations’ effectiveness to achieve the organisational goals”.
Table 2.4 shows the link between CS and risk management based on the above.

Table 2.4: Link between CS and Risk Management

CSRM		
CS Components	**Risk Management Application**	**References**
Information systems security	Safety in the information technology resources of the organisation. Determining potential risks and their impacts on information resources.	Hoffman, Kiedrowicz and Stanik (2016)
Human management	Risk identification, assessment, and mitigation of security threats by humans and could also constitute a threat source.	Ani, He and Tiwari (2019), Hadlington (2017)
A strategic approach to organisational CS management	Provides a structured approach to managing organisational CS risk by providing management staff with the requisite information to make the right CS decisions.	Bissel (2013), CBN (2018), Chen and Duvall (2014),
Identification and performance of proper tasks which contribute to treatment and alignment of technical and social elements of the identified security risks and deficiencies with organisational objectives.	Qualitative and quantitative analyses/assessment of risks results in quality decision making towards CSRM success.	Tisdale (2016), Meszaros and Buchalcevova (2017)
Design and implementation of appropriate controls. These include the formulation of security policies and the application of security standards as both preventive and mitigative measures for CSRM.	The proper application of Risk Management principles, procedures. Precise analysis and understanding of risks critical to achieving effective CS within the organisation. Well-executed risk management directly contributes to organisation effectiveness.	Hadlington (2017), CBN (2018)

Table 2.4 above shows that while CSRM is essential for organisations, effective risk management forms an integral part of organisation CSRM's overall strategy. Risk management provides an approach by which uncertainties/risks can be understood, assessed, and managed within CSRM. The risk identification and assessment of the risk management process form an essential part of a decision-making process towards choosing the appropriate CS method. Rational organisations would focus their limited resources on those areas that truly differentiate CSRM implementation success and failure. To support introducing and implementing a successful CSRM, formulating explicit and understandable policies by the management staff is indispensable. Communicating such security controls ensures all employees understand the CSRM process within the entire organisation.

2.5.1 Risk Management Process and CSRM Frameworks

The risk management process has become the main driving force for creating CSRM strategies, building risk management and security road maps, prioritising risk management activities and choosing protection and safety measures (Hoffmann, Kiedrowicz and Stanik 2016). The risk management process as a continuous re-iterating process consists of coordinated activities such as risk identification, assessment, treatment, selecting the best response, implementing mitigation actions, controlling and risk monitoring (McShane, Eling and Nguyen 2021).

Risk management entails utilising proper steps or clear procedures to eliminate or reduce the organisational risk to a reasonable level (Kendrick 2010). Each of the processes and components of risk management plays a vital role in an organisation's CSRM implementation efforts and success (Hudin and Hamid 2014) in achieving good governance and corporate objectives (Althonayan and Andronache 2019; Institute of Internal Auditors 2013). Authors define risk management in subsection 2.4.2, but practice and successful implementation are understood and interpreted differently using risk management frameworks as blueprints. Cyber security risk management exceeds selecting security controls but involves a multi-dimensional decision-making process to identify, select, implement, and monitor proper controls.

Literature consists of many risk management standards/frameworks for CSRM, broken into three major groups. One, standards (e.g., the ISO 27001 series); two, CSRM frameworks based on best practices (e.g., NIST); and three approaches based on the latter developed by various researchers and organisations (e.g., to address the limitations of other generic approaches). A representative of such frameworks' core phases is discussed below based on their broad applicability (AIRMIC and Irm 2010).

2.5.1.1 Risk Identification

The organisation's starting point is to obtain information about the specific objectives and assets at risk. To formulate the risk management strategy, an organisation must proactively identify the threats and vulnerabilities that may affect its objectives (McShane, Eling and Nguyen 2021). Risk identification can be in two contexts: internal and external context (Sadgrove 2016). The environment in which an organisation operates represents the external context. These include the economic, political, and social environment. The internal context includes governance, people, operations, and finance (Sadgrove 2016).

Recognising and expressing each risk factor is essential for risk identification. Several risk identification methods include Brainstorming, focus groups, Strength, Weakness, Opportunity and Threats (SWOT) analysis, audits, systems analysis, scenario analysis, failure analysis, risk identification forms, checklists, accident investigation, communication and feedback (Kikwasi 2018). Cyber security audits help identify different vulnerabilities and suggest remedial measures (Islam, Farah and Stafford.

2.5.1.2 Risk Assessment

Next to risk identification is an assessment that involves an in-depth analysis of the likelihood of risk occurrence and its organisational impacts (Ionita 2013). These impacts could affect the organisation's reputation and the ability to compete effectively in the marketplace. A risk matrix or risk map presents risk magnitude and likelihood (or probability) in an organisation in different formats. Still, its broad applicability in the CSRM domain as a valuable tool for risk assessment is daunting as more CS researchers and practitioners move toward more quantitative risk assessment methods (Hubbard and Seiersen 2016; Rios Insua et al. 2021).

None of the qualitative and quantitative risk analysis techniques is without criticism (Aven 2012; Aven and Zio 2014). Examples of quantitative techniques in the CS domain include probabilistic risk assessments, Bayesian methods and System ideas - Modelling Technique-Sensitivity Analysis, Scenario Technique–Monte Carlo Simulation, Diagramming Technique-Fault Tree Analysis and Event Tree Analysis (ETA) (Vose 2008). Qualitative approaches include brainstorming, interviewing, Delphi technique, checklists, Preliminary Hazard Analysis (PHA) among others (Rahman and Al-Shaer 2013).

Risk management continues to gain ground in a dangerous world. The preventive next-generation CS risk assessment and management approaches move towards the decision-analysis-led CSRM approach less 'one-size-fits-all'. More tailored and tiered risk assessment triplets (threat, vulnerability and consequences) for quality detection and appropriate solutions (Ganin et al. 2020; Maisey 2014).

2.5.1.3 Risk Evaluation

The evaluation step is to review the analysis and quantify its risk impacts. The aggregation will help the organisation to identify their risks, make the right decisions and the appropriate method to manage the risks (Sadgrove 2016).

2.5.1.4 Risk Treatment

Risk treatment changes the probability of any negative and positive consequences (Purdy 2010). This process is cyclical and essential for taking corrective measures peradventure risk responses deviates from the expected outcomes (Sadgrove 2016). Risk treatment ensures that the risk response is implemented and monitored for effectiveness (Sadgrove 2016). The monitoring entails costs and benefits analysis, prioritising and implementing the chosen treatment through a systematically planned process (Purdy 2010). The common risk responses include:

- Avoidance: This approach can be achieved by not starting events that could lead to uncertainty and high risk.
- Acceptance: Taking risks when the identified risks are within tolerance level with little or no considerable impact on other interrelated activities or the organisational success (Purdy 2010). Risks may be accepted to pursue an opportunity.
- Reduce/mitigate: Dealing with negative consequences that can affect objectives (ISO 2009).
- Transfer: sharing the risk with a third party considered better in managing the risk (Mukhopadhyay et al. 2017).

2.5.1.5 Communication and Consultation

Communication and consultation must be a continuous process throughout the risk management process. For risk management to succeed, there is the need to consult and engage the stakeholders (external and internal) for their inputs into the process and output ownership. Understanding stakeholders' objects are pertinent in setting the risk criteria to plan their level of involvement, and their views can be considered (Purdy 2010).

2.5.1.6 Monitoring and Review

Monitoring and review follow after implementing a risk control. Monitoring and review are crucial to ensuring that the adopted risk response strategies and controls are adequate, review lessons learned and appropriately manage the organisation's risks to be resilient (Collier et al. 2014).

2.5.2 Summary

The process of risk management shows the continuous and iterative processes involved. It is supposed to be an integrated component of CS. Therefore, risk management should adapt to risk and correspond with the technology system unfolding. Firms need to have a technical and non-technical capability to mitigate risk, as it appears. It is noteworthy that despite the various solutions and advancements to manage organisational processes and functions, inappropriately implemented CSRM would result in a high CSRM failure rate, challenge business growth and erode corporate values (Chabinsky 2014).

The prevalence of emerging CS risks further strengthens the need to engage in agile and reliable processes to mitigate the challenges of risk management and CSRM approaches. Therefore, there must be a continuous balance of prevention, detection and response to risk management activities across technology systems (Soomro, Shah and Ahmed 2016; Touhill and Touhill 2014). Risks, including CS risks, might be challenging to prevent and entirely eradicate but mitigate the detrimental effects. Risk managers, security practitioners and policymakers are under compulsion to identify and understand the inadequacies in current risk management methods and practices, match the emerging trends and catalyse efficient solutions or responses to mitigate evolving CS risks, attacks, and threats.

Many studies have studied CS/information security implementation challenges (Fenz et al. 2014; Kosub 2015). These challenges and the successive failure to implement CSRM underpin the importance of understanding and evaluating the factors associated with a successful implementation of CSRM. The balance between managing CS risks and risk management from the review of some journals, articles present asking the question ‘what factors influence CSRM implementation success?’ Current academic and industry literature must be well-read, synthesised and analysed to critically investigate the success factors influencing CSRM to address this

question. The following section describes the literature review process of the success factors for CSRM and the findings.

2.6 Literature Review Process

The important feature in all research is the literature review. A literature review generally provides an overview, synthesis, and critical engagement with previous research, identifying a problem or challenging existing knowledge and formulating new or likely research questions that lead to more prominent theories (Alvesson and Sandberg 2011). This research's literature review transcends summarising and quoting references but critical engagement with literature and what it means to be scholarly in academic work through an extensive overview of the success factors for CSRM in related extant literature. Finally, critique and summarise prior studies to identify where the current research can contribute to a knowledge gap in the literature and produce a comprehensive success factors model for implementing CSRM in large organisations in Nigeria. The research problem was defined before the commencement of the review. Appropriate guidance from academic experts helped focus the careful selection of relevant literature.

After developing the IS success model, many research topics have been on success factors and models. This research benefits from the comprehensive literature review. It summarises the success factors in both singular and organisational contexts of prior research in CSRM and its related fields to focus and understand the success factors for CSRM implementation.

The review type chosen summarises the findings of various coherent, relevant CS/CSRM studies and a review of applicable relevant theory. The aim is to create study predictability using the information gathered from previous studies as inputs for this study. It then identifies new success factors added to the list of known success factors, forming the input for the future CSRM implementation success in organisations.

The method is among the well-established approaches to assess cumulative knowledge and integrate research findings within a domain. It provides this research with a broad topic context, highlighting the importance of a novel study. Therefore, it is imperative to cut across vivid debates among academics, practitioners, and various research methods, which assisted in choosing appropriate research methods that help address the research objectives, as explained in the next chapter—the critical literature review (Wallace and Wray 2021).

Four reasons embellished for adopting a critical literature review to understand and improve the literature's current knowledge in this domain. One, both qualitative and quantitative research can be analysed and evaluated to conclude the CSRM domain's state. This does not suggest that the need for mathematical (quantitative) evidence to CSRM research is no longer necessary. Nevertheless, studies of qualitative evidence can add value to the important role of systematic reviews of practice, policies and strategic decision-making that might benefit CSRM implementation managers. Two, analysis can incorporate previous studies that do not use qualitative methods or report enough information in a meta-analysis. Individuals at different levels of management and organisations view success differently and can have different classifications of success factors in qualitative and implementation research. Three, examined the specific variables that influence the previous security success model and extended models in IS research. Perhaps close the gap between CS research and respond successfully to the persistent emergence of many CS challenges organisations face and faulty CSRM implementation practices. Four, the overall evaluation of CSRM implementation success factors formed due to this review are consistent with and extend beyond the standard quantitative methods employed in some previous research but qualitative experience and interventions that directly inform practices.

This study examines research published during the 15 years between 2006 and 2021. This research review examines the literature on success factors from various perspectives. The review process details to answer the question- what factors influence CSRM implementation success is below. Electronic tools to search for and select related published studies on CSRM success supported the process. Full-text searches in numerous online databases given in Table D1 (see Appendix D) use multiple keywords, such as ‘Cybersecurity risk management success’, ‘Cybersecurity risk management effectiveness’, ‘success factors’ and ‘critical success factors, ‘risk management’, ‘Cybersecurity’ and ‘cyber risk management’.

Using these Databases in Table D1 allows access to scholarly and peer-reviewed articles written by experts and reliable authors to ensure that the bibliography of relevant studies was complete. The review examines print issues of well-known information security journals unavailable electronically to ensure the inclusion of related studies and the exclusion of book reviews and editorials. Only papers reporting empirical results (both qualitative and quantitative) of various success factors and interrelationships among different success dimensions are included in this study.

Furthermore, repeated the search by adding the specific word 'Nigeria' to these keywords to cover relevant literature specific to the Nigerian context. It is essential to review much of the relevant literature for conducting a good literature review. However, because the study's reference discipline is management, this research focuses on factors that enhance CSRM implementation success to avoid being overwhelmed. Within the CSRM-related discipline, journals constitute the main literature search, knowing that several other relevant fields often research cybersecurity /information security success factors (Health, Accounting, Psychology, but to a lesser extent). However, the literature review is not restricted to a specific use context (private or public, organisational, or individual contexts), proving that this phenomenon is robust.

After examining over 700 articles resulting from any combination of the keywords initially skimmed for further processing, attention focused on synthesising and integrating empirical and conceptual studies judged valuable and relevant for the extensive search for CSRM implementation success factors. The review of these studies' output summarised the literature on success factors influencing CSRM implementation. A spreadsheet helps capture the information from these studies and categorise the factors.

2.7 Prior Related Works in CSRM

An increasingly topical issue that resonates in organisations' agenda is evaluating CSRM implementation's success or failure. Organisations need effective CSRM implementation for protection from cyber risks and breaches. Managers are always under the pressure of high costs of implementing and maintaining security controls (Chatterjee 2019). Hence, decision-makers must prioritise the organisation’s controls of significant importance (Diesch, Pfaff and Krcmar 2020). Smart organisations would channel their scarce resources on those factors that differentiate between failure and success (Bednar and Welch 2019).

Understanding the word ‘success factors’ is fundamental in the security genre. Studies globally have acknowledged success factors in different ways as a basis for managing risks, including CS risks. The term success factors continue to be significant to cybersecurity/information security managers, security policymakers and implementation managers. However, CSRM success factors could be elusive, as different people have various meanings and interpretations of what constitutes success (Agarwal and Rathod 2006).

- **Taxonomy of Success Factors and Selected Studies.**

Success is defined as achieving the goals established for an undertaking (Petter, DeLone and McLean 2013). The taxonomy of success factors has different forms of expressions across multiple contexts as management measures. Rockart (1979) defines critical success factors as the limited number of areas in which satisfactory results will ensure the organisation's successful competitive performance. Some researchers endeavour to study management requirements for information systems and other application disciplines by comprehending the 'professed' critical success factors or success factors. For example, strategic planning is a key activity area where favourable results are essential to reach organisational goals (Bullen and Rockart 1981).

As selected key result areas in construction risk management, an organisation must determine and implement amid risks to achieve its overall goals and objectives (Kikwasi 2018). In risk management systems, as essential success factors for readiness, implementation, and administration (Yaraghi 2011). In security risk management, critical success factors are descriptors and perceptions of accomplishing the effectiveness of security risk management programmes (Zafar 2011). In project management, as key success factors or real success factors and behavioural predictors of success (Camilleri 2016). In financial industries, success factors are E-banking fraud prevention (Usman 2013) and variables that influence information systems success (Petter, DeLone and McLean 2013).

These definitions identified four crucial areas: activities, variables' choice ('success factors'), the organisational context, and the study's objective. However, success factors are essential components in the CSRM field currently lacking within the next few years at the organisational level. It is unlikely that evaluating a single success factor could be sufficient for such a multidimensional concept of CSRM. Since success factors seem inevitable for implementation success and organisational performance of security analysis at the enterprise level (Ram, Corkindale and Wu 2013), this study extends it to organisational CSRM implementation success in Nigeria. According to this study's knowledge from the literature, there is a lack of a conceptual model for CSRM implementation success factors.

- **Holistic View of Success Factors for CSRM Implementation**

In section 2.5, the conceptualisation of CSRM provides clarity to the exploration objective and process. Exploring factors that influence CSRM implementation success needs a holistic view of

the organisation because the cyberwar requires enterprise-wide initiatives and efforts to protect the numerous vulnerabilities and endpoints. Combining the literature review in CSRM and other related disciplines is the foundation for identifying and evaluating CSRM implementation success factors.

It is necessary to ensure that CS activities incorporate information security in an organisation. Since CS has a link with information security (Öğüt, Raghunathan and Menon 2011), organisations must define and ensure security threats and vulnerabilities to information resources. The role top management plays (Ogoh 2016), the awareness, enforcement and maintenance of information security policies form the non-technical prerequisite for effective cybercrime management and information security in Nigerian banks (Okolo 2016).

The critical success factors approach identified ten fraud prevention factors in e-banking in Nigeria under the broad theme of strategic, technological, and operational factors (Usman and Shah 2013). From a different perspective, few studies review and argue that implementing risk management strategies did not receive a due reference by identifying the failure factors from financial distress in the financial sector (Dugguh and Diggi 2015). Although this study addressed essential issues, it focused on the financial risk management context but failed to evaluate an organisation's comprehensive view from the CSRM context.

Risk management decisions are so diversified that they are not limited to financial decisions and ensure CS decisions of risk identification, assessment, evaluation, response, and monitoring are successful (Dionne 2013). Financial measures often yield quantitative figures capable of convincing top management and decision-makers to invest in information technology (Nazareth 2015). However, cost-benefit analysis and Return On Investment (ROI) analysis are not complete solutions since no inherent methodology successfully measures security levels (Martin, Bulkan and Klempt 2011). This is just a means to an end, but the risk management principles can be applied in the CS context for CSRM implementation success.

In contrast, a further study narrowly evaluates security risk analysis and management of information security risk associated with a low level of awareness of financial clients and calls for research to evaluate security risk management associated with information technology platforms (Gana, Shafi'i and Ojeniyi 2019). Both studies (Dugguh and Diggi 2015; Gana, Shafi'i and Ojeniyi 2019) assert that proper risk management practices can lead to customer satisfaction, growth, and profitability in Nigeria's commercial banking sector. In agreement with Hoyt and

Liebenberg (2011), without much doubt, the banking sector constitutes the largest sector in Nigeria and the primary adopters of the advantages of internet services and more challenged.

A capable board is a foundation for an effective corporate governance system. Corporate governance is the most crucial driver in risk management adoption and implementation in large public listed companies in Malaysia (Manab and Hussin 2010). Similarly, 48 financial institutions' firm performance in Nigeria highlighted a significant positive relationship between corporate governance practices, risk management strategies and firm performance (Effiok, Effiong and Usoro 2012).

In Nigeria, several studies evaluated the cybercrime and CS issues and challenges among e-retailers (Aminu 2013). Others considered the use of security policies, Acts and strategies for sustainable CS (Osho and Onoja 2015; Saulawa and Abubakar 2014), citizens' education, advanced technology software, hardware and cyber legislation laws as solutions to these numerous CS challenges. A few studies drew attention to little or no significant success of CS implementation measures (Achumba, Ighomereho and Akpor-Robaro 2013; Makeri 2017; Oforji, Udensi and Ibegbu 2017).

- **CSRM Analysis Models**

The socio-technical analysis of cybercrime and CS in a government institution in Nigeria concludes that the sincerity of rigour of implementing and administering measures such as information technology security and intelligence, policies enactment and law enforcement will effectively and efficiently reduce CS risk (Olayemi 2014). In contrast, findings from game-theoretic models for the analysis of CSRM emphasise the use of resources, information sharing, internal controls, technical improvements, behavioural or organisational scale-ups and cyber insurance for CSRM (Akinwumi et al. 2017). Further reveals that game-theoretic models are still in their developmental stages with attendant limitations of much improvement needed. The game theory fails to recognise the essence of the part dependence of industry dynamics (Miller, Greenwood and Prakash 2009), with shared knowledge assumptions inapplicable in cybersecurity (Rios Insua et al. 2021)

More recent evidence, Ogu, Ogu and Oluoha (2020), justifies and proposes adopting a feasible, operational, and unified global CS legislative framework that is presently lacking to enhance CSRM implementation success that promotes cyber peace. However, most of these studies have

generally addressed CS at a national level but not at the organisational level. Further investigation of Nigeria's financial institutions posited a 38% adult banking population because some institutions are yet to deploy strategies to mitigate cyber exploitations (Alawode 2020). The thematic analysis of six CISOs of financial institutions concludes that a comprehensive risk management process incorporating aligned corporate strategy with information security plans, security policies, processes and procedures determine information security strategies that prevent cyber exploitations (Alawode 2020).

These studies further confirm the literature gap and the need to explore the success factors for CSRM implementation in large organisations in Nigeria to deliver significant benefits to clients and the organisation. Cybersecurity risk management implementation success and realization are not automatic. The multi-dimensional and interdependent nature of CSRM shares some standard features with information systems, information security, information security risk management (Jung 2011; Safa, Von Solms and Furnell 2016).

Since cybersecurity risks emanate from the in-depth penetration of ICT devices and IT systems into business operations, organisational factors classified into three levels: strategic, operational, and tactical, are necessary for information security management issues (Singh 2014). These factors include security policy, asset classification and control, organisational and personnel security, communications and operations management, physical and environmental security, system development and maintenance, access control and business continuity. In contrast to the previous study findings, similar studies of the organisational factors impacting implementing information security management revealed different factors such as environment uncertainty, industry type, IT competence of business managers and organisation size (Chang 2006; Perez 2013).

The success factors for enhanced information security implementation in government organisations in an underdeveloped country, Oman, were identified in a case study (Al-Awadi and Renaud 2007). Findings from the semi-structured qualitative interview data reveal that top management provides adequate financial resources to acquire necessary employees awareness and training on security issues, acquisition of skilled human resources and efficient technology, adherence to policies and regulations. The findings suggest that the identified factors are interwoven; hence, ascribing a certain level of priority or criticality to a factor will be problematic and challenging.

Likewise, implementing cyber/information security policies through employee engagement in practice is directly proportional to enhancing a functional cyber risk-free organisation (Siponen, Mahmood and Pahnila 2014). Cyber/information security policies need to integrate with the organisational strategy and technological solutions as governance, risk, and control tools for effective CSRM (Nicho, Khan and Rahman 2017; Safa et al. 2015).

Considering the high dependability on the availability of information systems in achieving the business goals and objectives, twelve critical success factors grouped into three levels of controls are necessary for managing information systems security (Torres et al. 2006). These include technology/technical controls (proper introduction, protection and use of hardware and software business connections and structures to restrict unauthorised access and incorrect use); informal/people controls (interventions that enhance digital information security by improving workforce will power and willingness such as awareness, staff confidence and management commitment); and formal/process controls (set of procedures and policies to establish and ensure effective use of technical controls.

The balance of these controls must be equally and dynamically implemented and managed to achieve CS success. Neglect of any of the three security controls could result in CS failure. This study is consistent with the submission of (Al-Awadi and Renaud 2007). It predicts that the future of information security needs a holistic approach based on the dynamic balance between technology, processes, and people. This aligns with Mitnick and Simon (2011) submission that CS is a process and not a technology problem but a people and management problem.

Through qualitative, content analysis of six related studies, the success factors and elements that contribute to efficient information security management practices were grouped into three main aspects- People (Top management leadership and commitment, knowledge, skill and commitment of ISM team and audit team, employee awareness and motivation), Process (Risk management, IS audit, human and financial resource planning, competency development through awareness and training programmes, business continuity through test and planning) and Organisation (IS policies and procedures) (Zammani and Razali 2016). These factors are typical of Torres's study, and business continuity management and IS audit are added as ISM success factors. Business continuity management plans were drawn through risk assessment and business impact analysis to ensure resilience as a security star in managing and controlling any adverse security incidents.

Further advanced quantitative studies made explicit the critical success factors for the strategic value alignment for information security management at an organisational level using a balanced scorecard model (Tu and Yuan 2014; Tu et al. 2018). These factors grouped into four levels, including organisational support (organisational structure, the commitment of resources and top management support), organisational awareness (staff awareness and training, information security culture), business alignment, IT competence and Security Controls (risk management, security policies implementation, standards application). In a narrow view, the combined commitments from management and implementer competency influence the Information Security Management System plan phase self-implementation in the Malaysian government sector from a qualitative perspective (Maarop et al. 2015).

The business and security needs must match every IT activity to achieve security success using the three control groups: operational controls such as physical security, backup and incident handling and response; strategic controls-business alignment and governance; risk and compliance; and tactical controls, for example, secure builds, antivirus, and intrusion prevention (Bunker 2012). In a significant advancement, scholars argued how various alignment dimensions, including business strategy-IT alignment of environmental and organisational factors in developing countries (Yayla and Hu 2012) and business-IT alignment (Gerow et al. 2014), achieve security success. Their analyses have not received general acceptance. An alternative explanation suggests that understanding the strategic alignment's complex nature positively affects corporate settings and improved performance (Coltman et al. 2015).

Subsequent studies found the need for several dimensions of business-IT alignment, including strategic/intellectual alignment, structural alignment and social alignment of high relevance for organisational success (Schlosser et al. 2015; Ilmudeen, Bao and Alharbi 2019), as an innovative approach. The social aspect of alignment represents the relationships and shared understanding between the three units. Karpovsky and Galliers (2015) noted identifying and classifying the dynamic factors of aligning activities in practice in the real-day hyper-connected world is a new research theme relevant for IT/IS-business alignment for organisational CSRM success. These factors include enablers (governance practices) in conjunction with dynamic actors (top management and IT competencies) and controlling parameters of budget control and monitoring amongst others.

- **Risk-Based CSRM**

Risk management as a success factor can help better identify and understand significant complex problems of CS and stimulate the decision-makers to make better-informed decisions of improvement policies, eliminate financial risks of over or under budgets through timely internal feedback mechanisms. Much extensive empirical research has evaluated risk management's contribution, especially in IT project success because of the nuance of IT project failures (de Bakker, Boonstra and Wortmann 2010) and overall organisation's CSRM (Althonayan and Andronache 2019; McShane, Eling and Nguyen 2021). Some concluded the need to rethink the socio-technical factors that influence enterprise risk management implementation for success (Jean-Jules and Vicente 2020).

It is thought-provoking to see others classify the strict application of risk management processes and procedures as the bedrock of successful information security risk management (Hoffmann, Kiedrowicz and Stanik 2016; Nather 2018). Some researchers apply risk management tools and techniques to improve the information security management system (Maarop et al. 2015), IT project risk management (Javani and Rwelamila 2016; Zwikael and Ahn 2011) by establishing a project management office to manage the implementation process.

The evaluation of risks and risk assessment tools and methodologies (Aviad, Wecel and Abramowicz 2018; Ganin et al. 2020) led to various approaches that resulted in the adjustment of the use of the methodology or the adaptation of the method itself in CSRM (Collier et al. 2014; Meszaros and Buchalcevova 2017; Rios Insua et al. 2021). Implementing risk management success factors is efficient, effective and efficacious (Hopkin 2017). An organisation achieves the enterprise risk management value when the top-management approaches strategically embed and aligned risk management activities to all aggregated current and emerging risks with IT governance and risk culture to achieve the organisational objectives (Mayer and De Smet 2017).

The need to identify critical factors to successfully run, maintain and administrate Risk Management Systems (RMS) implementation found factors grouped into five broad components: a well-defined strategy, human resources, top management support, organisational culture and structure in Swedish Corporations using grounded theory and survey (Yaraghi and Langhe 2011). Although the identified factors could be expected in most organisations, the study focused on successful Swedish companies with a relatively small sample. Further recommendations call for broader sample sizes in other organisations and sectors in more geographic borders. A case study

of a construction company in Tanzania identified nine composite critical success factors for effective risk management (Kikwasi 2018).

These risk management studies' discoveries provided the impetus for further research on applying risk management success factors in the CS field. One could not ascertain if the factors are suitable for CSRM implementation in large organisations in Nigeria due to personnel's distinctive characteristics, working practices and cultural issues common in implementation projects (Choudrie et al. 2017). Extant literature and many organisations adopt CSRM standards, frameworks, and best practices to address other generic approaches' limitations as a starting point to establish CSRM strategy (Beasley et al. 2020; Kosub 2015). These standards, for example, the NIST CS framework and the variants of International Organisation for Standardization (ISO) standards, suggest appropriate guidelines, checklists and security controls that could be implemented for managing CS risks (Evans 2016; NIST 2014).

In advancing the above stance, cyber governance, situational awareness, resilience, and risk management have become business management functions for top management a long time CSRM control of strategic, tactical, and operational levels services and communications of large organisations using the combinations of six available standards as the framework (Verkerke 2015). Unfortunately, Verkerke's approach has neither received general acceptance nor escaped criticism from the case organisation as inconclusive. Hence, the findings suggest conjectures based on ambivalent assumptions searching for further evaluations. Although the adoption of standards and frameworks presupposes that certificated organisations are committed to CS, this is hard to crack in implementing such standards/frameworks. However, CS standards can provide valuable elements of a cyber-approach and help organisations participate in the complex cyberspace with no silver bullet solutions in a responsible way (Verkerke 2015).

More importantly, in the security of confidentiality, availability and integrity of business information, risk management, the standards serve as blueprints for the practice and successful implementation of CSRM. These blueprints help organisations integrate CSRM into daily functions and activities (Shackelford et al. 2015) since individuals will have input or implement any risk management system. These individuals' attitudes to risk could significantly impact the successful implementation and management of CS risks in the future. Organisations implement these numerous CSRM frameworks to help identify, detect, protect, respond and recover from cyberattacks to address the enterprise CS challenges (Gourisetti, Mylrea and Patangia 2020).

- **Human-Business Management Views**

A holistic view of a security matured organisation identified six critical success factors for an effective security risk management programme (Zafar et al. 2011). This requires a focused corporate security strategy that revolves around executive management support, open communication, implementation of security policies among risk management stakeholders and human resource development/team member empowerment. The above suggests that clear security roles, responsibilities, and requisite knowledge of determining risk tolerance are catalysts to implement acceptable preventive and mitigation responses (Trim and Lee 2014). Thus, embracing the concepts of corporate governance and enterprise risk management is a critical component for CSRM implementation (Allen et al. 2018). This argument aligns with the study that reckons to apply corporate governance as an excellent way of managing CS risks (Bobbert and Mulder 2015).

Suggesting a pathway to CSRM, most studies focus on technology; CSRM demands new thinking towards the assets to be managed beyond the fundamental technology processes (Chabinsky 2014). Previously, CS research centred on security around the information security perimeter fence which does not work in isolation (Ahmed and Matulevičius 2014; Masky, Young and Choe 2015). More research into the socio-technical elements of CS is imminent (Jean-Jules and Vicente (2020).

Organisational, interpersonal relationships, leadership involvement in CS decisions, agile knowledge transfer and effective risk management are among the top factors for CSRM implementation success (Tisdale 2016). Strengthening organisational security awareness of CS risks and improved security controls with greater alignment between security risk management and the business environment positively impacted security risk management performance using system quality theory and buy-in theory (Spears and Barki 2010). Increased CSRM awareness, practical training and practices are crucial to increasing user participation, minimising common CSRM user-related faults, maximising the efficiency of security techniques, procedures, and controls instead of checklist dos and don'ts (Kennedy 2016).

Humans have become a central part of all the support systems as assets, threats, and vulnerabilities (Stewart and Jürjens 2017). Training in protective behaviour can mitigate many risky CS behaviours that impede CSRM implementation success (Gillam and Foster 2020). The importance of awareness and training ranges from compliance with policies to knowledge management of

various attack vectors and risk management control solutions which cannot be over-emphasised in CSRM implementation success (Flowerday and Tuyikeze 2016).

- **System Thinking Views**

A renewed school of thought recognises the importance and progression towards CSRM implementation success in a contemporary approach of purposeful activities of socio-technical and socio-economic elements and phenomena. Regarding CSRM implementation, it is critical to understand the relationships between the technical systems and humans operating them (Baxter and Sommerville 2011). Among many studies, Petter, DeLone and McLean (2013) found predictors (success factors) that influence IS success (dependent variable) as an extension of the original D&M model that has found broad applicability in CS, information security and other related fields.

These success factors organised into three of Leavitt's dimensions of Organisational Change: tasks, people and organisation structure and its effects on technology success seem ambitious for this study. The study identified the relationship between independent variables that influence IS success's specific dimension (Service Quality, System Quality, Information Quality, Intention to Use, User Satisfaction, System Use and Net Benefits) and its organisational environment. Important applicability of the model is the ability to help measure the success of implementation from various perspectives.

A prominent critic of this study is that, at best, it represents a macro view of the evaluation of value derived from total technology/IT investment. Although this study identified the success factors of IS success in which technology is a crucial component, this study does not provide details about how other factors influence CSRM implementation success. The extension of system safety from system thinking and system theory in CSRM in a retail organisation highlighted several success factors to prevent the future successful attack (Salim 2014). Since organisational CS risks differ, enterprise resources, the tools and techniques, processes, and structures necessary to achieve successful CSRM implementation against malicious CS attacks will be different (Craigen, Diakun-Thibault and Purse 2014; Dasso et al. 2016).

More recent evidence reveals the need for systemic thinkers emphasising the blend of social intelligence, technical and organisational skills that influence and dictate success or failure in everyday enterprise-wide settings (Dawson and Thomson 2018). Smart organisations design

effective tools, techniques, technology, processes, and human resources to achieve desired outcomes (Bednar and Welch 2019). Organisations require a common framework to ensure adequate security of systems and monitor their readiness to mitigate a series of attacks as a guideline to assess their existing CSRM implementation programme. They build frameworks from existing tools and standard controls to analyse the social, technology and environmental influences on organisational practices (Masike, Sune Von and Marnewick 2019).

- **Summary**

The current literature addressing success factors for CSRM in related fields are reviewed to understand and fill the gap between practice and literature in studying success factors that influence CSRM implementation. Thus, the review has revealed a taxonomy of critical success factors whose meaning and interpretation depend on the individual study and the organisational contexts. The thorough understanding of success factors in these related fields, existing managerial, organisational, operational, social and process factors, helped suggest the combination of unbiased factors that influence successful implementation of CSRM irrespective of the conjecture about their level of criticalities.

The literature review suggests socio-technical factors used in related cybersecurity research. The lack of empirical understanding makes it difficult to draw insights on how organisations conduct CSRM, what success factors and the nature of knowledge are required to mitigate large organisations' challenges in their CSRM implementation tasks and processes. Moreover, the vast literature account features that the maturity of CSRM implementation does not rely solely on a factor but needs a combination with several success factors. Thus, this study could introduce new factors that influence CSRM implementation success or adapt an existing system theme within the organisation's independent variables: tasks, people, technology, and structure for both technological and social changes according to Leavitt’s model. Table 2.5 below shows the eleven common success factors identified from the literature review.

Table 2.5: Success Factors Investigated in Studies for CSRM in the Literature

Dimension	Factor	Elements	Sources	Search result
Organisation	Business alignment	Incorporating the CSRM objective with the strategic objectives of an organisation	Amarilli, Van Vliet and Van den Hooff (2017), Atoum, Otoom and Abu Ali (2014), Coltman et al. (2015), Amarilli, Van Vliet and Van den Hooff (2017); Chang, Chen and Chen (2011), Gerow et al. (2014), Ilmudeen, Bao and Alharbi (2019), Karpovsky and Galliers (2015), Kayworth and Whitten (2010), Perez (2013), Petter, DeLone and McLean (2013), Salim (2014), Schlosser et al. (2015), Soomro, Shah and Ahmed (2016), Spears and Barki (2010), Srivastava (2017), Tisdale (2016), Torres et al. (2006), Tu et al. (2018), Tu and Yuan (2014), Wang et al. (2011), Coltman et al. (2015); Yayla and Hu (2012).	21
	Corporate governance	Promoting collaboration & CSRM culture environment among involved stakeholders	Allen et al. (2018b), (Andersen, Garvey and Roggi 2014), Bunker (2012), Chatterjee (2019), Dhillon, Tejay and Hong (2007), Dzazali and Zolait (2012), Effiok, Effiong and Usoro (2012), Islam, Farah and Stafford (2018), Karpovsky and Galliers (2015), knight (2006), Masike Malatji, Sune Von Solms and Marnewick (2019), Nicho (2018), Nicho, Khan and Rahman (2017), Torres et al. (2006), Trim and Lee (2014), Vincent, Higgs and Pinsker (2017), Zafar et al. (2011).	17
	Budget/ Investment	Factoring in the costs of CSRM resources within organisation budgets.	Al-Awadi and Renaud (2007), Chatterjee (2019), Disparte and Furlow (2017), Gordon et al. (2015), Gordon, Loeb and Zhou (2016), Srinidhi, Yan and Tayi (2015), Tisdale (2016), Torres et al. (2006), Tu and Yuan (2014), Tu et al. (2018), Zammani and Razali (2016).	11
People	Awareness	Awareness and knowledge of the process for implementing RM, awareness of CS threats and risks, compliance with policies.	Al-Awadi and Renaud (2007), Ani, He and Tiwari (2019), Disparte and Furlow (2017), Hussain and Skinner (2019), Kennedy (2016), Kraemer, Carayon and Clem (2009), Matthews, Arata and Hale (2016), Merete Hagen , Albrechtsen and Hovden (2008), Gjerdrum and Peter (2011), Ogoh (2016), Petter, DeLone and McLean (2013), Pfleeger and Caputo (2012), Shackleford (2016), Siponen, Mahmood and Pahnila (2014), Masike Malatji, Sune Von Solms and Marnewick (2019), Pfleeger and Caputo (2012), Puhakainen and Siponen (2010), Spears and Barki (2010), Tisdale (2016), Tu and	25

			Yuan (2014), Tu et al. (2018), Verkerke (2015), Weick and Sutcliffe (2007), Whitman and Mattord (2011), Zammani and Razali (2016).	
	Training	Inclusion of CSRM among education and training subjects of employees.	Al-Awadi and Renaud (2007), Chatterjee, Disparte and Furlow (2017), Hadlington (2017), Kennedy (2016), Kraemer, Carayon and Clem (2009), Pfleeger and Caputo (2012), Sarker and Valacich (2015), Puhakainen and Siponen (2010), Kennedy (2016), Schatz, Bashroush and Wall (2017), Siponen, Mahmood and Pahnila (2014), Srinidhi, Yan and Tayi (2015), Von Solms and Van Niekerk (2013), Wang, Nnaji and Jung (2020), Zammani and Razali (2016).	16
	Top management support	Support from managers, leaders, and commitment.	Chabinsky (2014), Chatterjee (2019), Disterer (2013), Gordon, Loeb and Zhou (2016), Harrison and Jürjens (2017), Karpovsky and Galliers (2015), Kayworth and Whitten (2010), Kikwasi (2018), NIST (2014), Perez (2013), Petter, DeLone and McLean (2013), Salim (2014), Schlosser et al. (2015), Spears and Barki (2010), Torres et al. (2006), Touhill and Touhill (2014), Tu and Yuan (2014), Tu et al. (2018), Wang et al. (2011), Wang, Nnaji and Jung (2020); Zammani and Razali (2016).	21
Technology	IT competence	Awareness, knowledge, and the capability of implementing CSRM	Bendovschi (2015), Chang et al. (2011), Chang and Ho 2006), Chang, Chen and Chen (2011), Dzazali and Zolait (2012), Jean-Jules and Vicente (2020), Masike Malatji, Sune Von Solms and Marnewick (2019), Perez (2013), Spears and Barki (2010), Kotulic (2001), Rivard, Raymond and Verreault (2006), Usman and Shah (2013).	13
	System quality	Availability and reliability of Technology	Bharati and Chaudhary (2006), Bendovschi (2015), Lyytinen and Newman (2008), Petter, DeLone and McLean (2008), Petter, DeLone and McLean (2013), Spears and Barki (2010), Wang, Klein and Jiang (2006).	6
Process /Task	Risk management / standard application	Awareness and knowledge of the process for implementing CSRM, risk management tools and techniques	Allen et al. (2018), Althonayan and Andronache (2019), Ani, He and Tiwari (2019), Akinwumi et al (2017), Bannerman (2008), Bednar and Welch (2019), Bergström, Lundgren and Ericson (2019), Charitoudi, Konstantinia (2013), Choo (2011), Collier et al (2014), Chabinsky (2014), Charitoudi, Konstantinia (2013), de Bakker, Boonstra and Wortmann (2010), Dzazali and Zolait (2012), Disterer (2013), Dubois et al. (2010), Dunkerley and Teejay (2011), Dugguh and Diggi (2015), Gana, Shafi'i and Ojeniyi (2019),	68

			Galliers (2015), Goss (2017), Hadlington (2017), Haapamaki and Sihvonen (2019), Hagental (2008), Hubbard and Seiersen (2016), Hudin and Hamid (2014), Ifinedo (2012), Ionita (2013), Islam, Farah and Stafford (2018), Jung (2011), Kahyaoglu and Caliyurt (2018), Karpovsky and Javani and Rwelamila (2016), Jean-Jules and Vicente (2020), Kayworth and Whitten (2010), Kiedrowicz and Stanik (2016), Kikwasi (2018), Knight (2006), Kosub (2015), Lee (2020), Maarop et al (2015), Matthews, Arata and Hale (2016), Masike, Sune Von and Marnewick (2019), Mayer and De Smet (2017), Ma, Johnston and Pearson (2008), McShane, Eling and Nguyen (2021), Merete Hagen, Albrechtsen and Foster (2018), Meszaros and Buchalcevova (2017), Nather (2018), NIST (2014), Rothrock, Kaplan and Van Der Oord (2018), Safa, Von Solms and Furnell (2016), Saunders (2017), Shackelford et al. (2015), Shamala et al. (2017), Spears and Barki (2010), Salim (2014), (Singh, Gupta and Ojha 2014), Tisdale (2016), Torres et al (2006), Tu and Yuan (2014), (Touhill and Touhill 2014), Vakharia, Mishra and Kumar (2012), Verkerke (2015), Vincent, Higgs and Pinsker (2017), Webb et al (2014), Yaraghi and Langhe (2011), Zafar et al. (2011), Zwikael and Ahn (2011).	
	Security policies	Knowledge, compliance	Al-Awadi and Renaud (2007), Cheng et al. (2013), Dzazali and Zolait (2012), Flowerday and Tuyikeze (2016), Goss (2017), Mayer and De Smet (2017), Mikes and Kaplan (2014), Nicho, Khan and Rahman (2017), Ogoh (2016), Okolo (2016), Osho and Onoja (2015), Puhakainen and Siponen (2010), Singh, Gupta and Ojha (2014), Saulawa and Abubakar (2014), Siponen, Mahmood and Pahnila (2014), Safa et al. (2015), Shackelford (2015), Siponen and Willison (2009), Siponen, Mahmood and Pahnila (2009), Spears and Barki (2010), Torres et al. (2006), Tisdale (2016), Zafar et al.(2011), Zammani and Razali (2016).	21
	Security audit	Gaps in the CSRM implementation process and CSRM maturity levels	Christ et al. (2015), Ege (2015), Islam, Farah and Stafford (2018), Kahyaoglu and Caliyurt (2018), Lin et al. (2011), Merete Hagen, Albrechtsen and Hovden (2008), No and Vasarhelyi (2017), Onwubiko (2009), Yang (2011), Zammani and Razali (2016).	10

Table 2.5 above shows factors that occur frequently and are supported by empirical research evidence selected to establish a conceptual model of success factors for CSRM. These factors play an essential role in the CSRM /IS domain, broad in scope and covers many regions and sectors. This research identified eleven factors posited to influence the different dimensions of CSRM success from related contexts as some of the factors overlap with each other in the groupings. Three success factors (People, Process and Technology) were selected based on their frequent discussions in the literature and organised recurrence of the groups and their importance to security success in the various contexts (Al-Awadi and Renaud 2007; Torres et al. 2006; Zammani and Razali 2016). Also, these factors are in line with the taxonomy of Leavitt's diamond of organisational change: Process (Task), People (Actor), Technology and organisational dimensions previously extended in IS success factors studies, as shown in Figure 2.2.

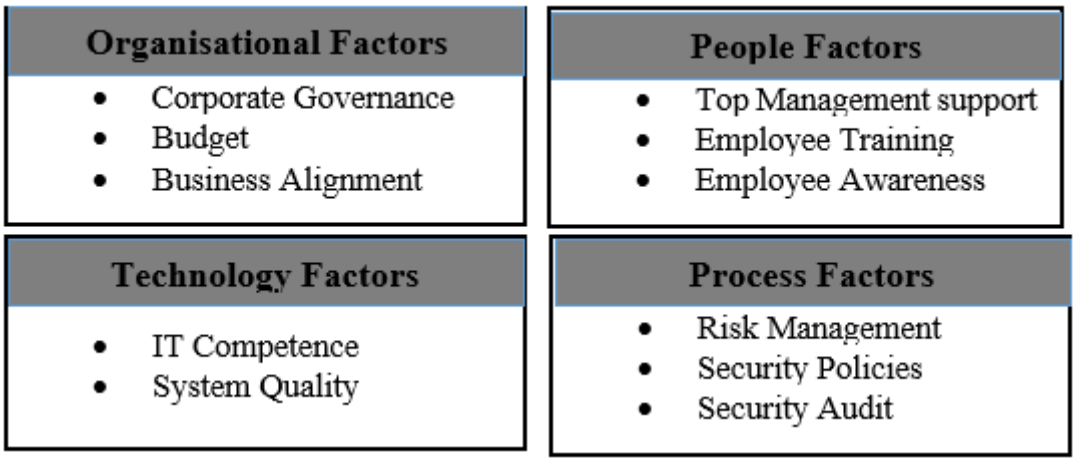

Figure 2.2: Top Cited Success Factors

These success factors and groupings have a broad scope from different organisational sectors from other geographic locations. These factors provide sufficient support for this study, extending the dimensions as a guide to explore success factors that influenced CSRM success in Nigeria in Chapter 5. The benefit of extending all the four dimensions as an exploration approach provided the needed consciousness of the interrelationships in disciplines and the factors influencing CSRM implementation. Each of these factors impacts differently, but equally, on CSRM implementation. Hence, integrating all the factors into a holistic approach is more elegant and practical to lead to successful CSRM implementation with apparent benefits.

2.7.1 Organisational Factors

Eliminating cybersecurity risks might not be feasible but sensible for organisations to prepare for their occurrence and ensure specific prioritisation for their management from the organisational context. The organisational factor is the social but management perspective that places CSRM within the organisational structure and the organisational strategy perspectives (Chang and Ho 2006; Perez 2013; Yaraghi 2011). The organisational structure constitutes the governance category, while the strategic perspective includes aligning CSRM within the broader corporate business goal (Bobbert and Mulder 2015; Dhillon, Tejay and Hong 2007).

The strategic perspective investigates the impact of factors that enable authority, communication and workflow on the successful implementation of CSRM at the organisational level (Singh, Gupta and Ojha 2014; Kumar et al. 2020). Also, the organisational factor consists of corporate strategy and organisational structure (Kayworth and Whitten 2010; Tisdale 2016; Tu and Yuan 2014). Others include strategically balancing the specific business needs (industry type, size and environmental uncertainty) with security needs through business managers' IT competence (Chang and Ho 2006).

Following are the three common organisational dimension sub-factors explained in Figure 2.3.

Figure 2.3: Organisational Factors

- **Business Alignment**

Business alignment is the process by which different aspects of the business organisation aligns to facilitate effective strategy execution to achieve CSRM implementation success and organisational objectives (Srivastava 2017). A strategically focused or business-driven CSRM implementation strategy is crucial and should align with the organisational goals for success (Spears and Barki 2010; Tu et al. 2018). This alignment leads to strategic CS moves that convert

CSRM implementation requirements into Specific, Measurable, Achievable, Realistic and Timely (SMART) and prioritised goals that drive the CSRM map into successful execution (Atoum, Otoom and Abu Ali 2014; Bednar and Welch 2019).

Thus, CSRM is a key business issue (Kayworth and Whitten 2010; Soomro, Shah and Ahmed 2016). This links with the business components of CS management: organisational governance and policy, CS investment planning and control, resource strategy and planning with the IT security components (Chen 2010). As an acquisition component and CS enterprise architecture, cyber security converts the strategic goals of CSRM implementation to execution performance (Tisdale 2016; Tu et al. 2018). The importance of alignment between two organisational dimensions (business-CS/IT alignment) becomes a success measure for evaluating effective organisational performance (Wang et al. 2011).

Scholars identified the multidimensional nature of related IT, intellectual and operational-business alignment dimensions relationships for organisational performance (Gerow et al. 2014; Ilmudeen, Bao and Alharbi 2019). The alignment is achieved through mutual understanding of the CSRM planners and the top management (Ma, Johnston and Pearson 2008; Wu, Straub and Liang 2015). The alignment helps create a formal CSRM implementation structure of co-evolutionary mechanisms of business-IT alignment managers at all levels are more responsible and willing to support sound CSRM implementation practices and successful organisational performance (Amarilli, Van Vliet and Van den Hooff 2017; Chang, Chen and Chen 2011).

When an organisation's CSRM strategy aligns better with the strategic business goals and objectives, its CSRM implementation will be successful (Spears and Barki 2010; Torres et al. 2006). Thus, business alignment facilitates organisational support for business-IT-related issues as a catalyst for broader and effective risk management plans and CSRM implementation efforts (Karpovsky and Galliers 2015). The knowledge and the interpretation of alignment mechanisms and the understanding of the compelling nature of the alignment process are considered key openings in alignment implementation success.

- **Corporate Governance**

This research defines corporate governance as the responsibilities and practices exercised by the board and executive management to provide strategic direction, ensure objectives achievements

and ascertain efficient cybersecurity risk management implementations through the appropriate and verifiable responsible use of organisational resources.

Corporate governance is a management and control function that creates and governs executing and monitoring CSRM implementation success through high-performance security culture with a proper chain of command established among dedicated teams or individuals carrying out CSRM activities or functions (Nicho, Khan and Rahman 2017; Nicho 2018).

Governance provides a balance of authority between the board of directors, the management and stakeholders, or understood as a set of actions conducted by the organisation and disseminated with various stakeholders' assistance (Oliveira et al. 2019). The stability and improvements of a company's CS performance are highly dependent on the active role of the interrelation between corporate governance risk management components (Allen et al. 2018; Islam, Farah and Stafford 2018). The organisational structure is a corporate governance category in a successful CSRM implementation (Allen et al. 2018a; Andersen, Garvey and Roggi 2014; Dhillon, Tejay and Hong 2007; Trim and Lee 2014). The information technology governance and strategic alignment for IT risk management practices and business performance (Vincent, Higgs and Pinsker 2017; Wu, Straub and Liang 2015).

Senior management's corporate governance structure leads the charge in establishing a CS culture of preparedness, joint ownership, commitment, responsibility, discipline and accountability in tandem with other organisational stakeholders that form the vital cornerstones of CSRM (Chatterjee 2019; Effiok, Effiong and Usoro 2012). Such corporate governance functions define the structure, strategy, methodology and performance measurements for CSRM implementation plans to identify, assess, monitor and mitigate organisational CS risks (Allen et al. 2018a; De Bruin and Von Solms 2016; Dhillon, Tejay and Hong 2007).

The corporate governance role is an element of management control that clarifies essential roles and duties by providing a simple and effective way to enhance risk management communication (Dzazali and Zolait 2012). In contrast, the risk management process develops the control environment (Dzazali and Zolait 2012). Therefore, corporate governance is the higher branch of the organisational structure that provides responsibility and accountability for efficient CSRM implementation. This glue binds an organisation to pursue organisational cybersecurity objectives while risk management offers CSRM implementation success resilience.

- **Adequate Budget Planning**

A successful CSRM implementation plan or programme needs appropriate financial support and budget level. Adequate budget planning means having sufficient, balanced financial support to meet the human capital resource needs, CSRM implementation activities and operations even when such investments seem not to be associated with revenue generation activities (Disparte and Furlow 2017). For any CSRM strategy to make sense and be effective, the costs and benefits of CSRM must be positively aligned with the associated risk, risk tolerance and not exceed or equal to the incremental investment cost and return on such investment (Gordon, Loeb and Zhou 2016.

Management must allocate sufficient budget to accomplish daily activities towards achieving both short and long term aligned CSRM implementation goals. CSRM expenses such as operational costs (e.g., maintenance, training and development), development costs (e.g., technology purchase and installation costs) and response costs (e.g., IT experts skills acquisition) should be perceived as opportunities to improve information security, information systems availability and reliability, necessary to ensure CSRM successful implementation that can threaten organisations existence but sustain organisational reputation (Chatterjee 2019; Torres et al. 2006).

Decision-makers must compare the opportunity cost of a breach over all the costs mentioned above and prioritise adequate budget planning/financial resources as a strategic management competence and an informed decision for successful CSRM implementation operations and processes (Al-Awadi and Renaud 2007; Zammani and Razali 2016).

2.7.2 People Factors

Cyber security risk management requires certain areas of expertise, variations of skills, knowledge, competencies, business, and risk management operations that cannot operate in a vacuum. CSRM must transcend the traditional silo risk management but includes a cross-functional assessment and understanding of how CS risks are connected and consider other related aspects, key players and expertise in managing CS (Kendrick 2010; Zammani and Razali 2016).

CSRM implementation needs many people (the social network) to work in one direction within the organisation system. The people factors theme in this study refers to those associated with stakeholders possessing requisite knowledge and skills for effective and efficient CSRM functions that make CSRM implementation successful in the organisation. These stakeholder

groups include organisation's employees who must be given adequate training and awareness-raising materials and programmes to safeguard security /information assets (Chatterjee 2019; Chatterjee, Sarker and Valacich 2015).

People are the central part of all supports system (Harrison and Jürjens 2017). CSRM initiatives need to be driven, supported and implemented by agile, competent, motivated and aware people (Maarop et al. 2015). Any CSRM programme will have input from or be implemented by people (individuals) whose attitudes to risk and diligence could significantly impact the successful implementation (Hadlington 2017; Shackelford 2016). It is a widely acclaimed fact that cyber-attacks exploit people's vulnerability (Bendovschi 2015).

Awareness, training, top management support resonate in the literature review among three relevant people dimension sub-factors for cyber/information security risk management, as shown in Figure 2.4. Although these stakeholders groups have defined roles and responsibilities, this study focuses on management tasks that interact through utilising resources and are structured into actions and operations to meet CS needs. This study reckons that the business issues and CSRM initiatives, investment in technology and controls and implementation can be successful if supported and sustained by human aspects of the organisation (Chabinsky 2014; Harrison and Jürjens 2017). An inquiry into implementing an effective management process of the individuals' attitudes, risks they face, and their decisions could help meet CS business needs and future CSRM implementation success.

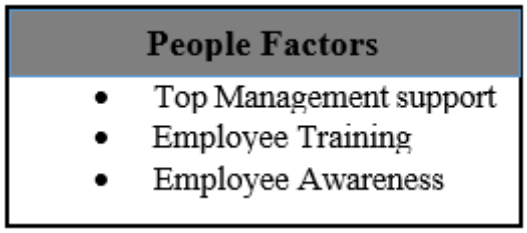

Figure 2.4: People Factors

- **Top Management Support**

Top management support means a commitment for CSRM implementation success from the management. Protecting confidential data and related digital and human assets is a business reality that is crucial to organisational CSRM survival and success. The continual corporate dependency

on information systems, information security, thriving in the competitive business environment necessitates top management commitment and support to drive technical and operational business decisions that enhance CSRM implementation success (Torres et al. 2006).

Top management support ranks among the first in most studies in all organisations in effective CSRM (Kikwasi 2018; Zammani and Razali 2016). At its highest levels, the tone, leadership, and commitment towards CSRM must come from top management commitment with clear organisational mission, security goals, and objectives (Al-Awadi and Renaud 2007). Top management plays a crucial role in working with various teams and stakeholders to formulate comprehensive and transparent CSRM policies communicated to all employees and stakeholders. Policies institute appropriate behaviours in the use, handling, unauthorised access to organisational resources and technology to facilitate CSRM implementation processes.

Apart from the fact that top management support is a requirement in CSRM standards, mandated by ISO 27001 standard (clause five on leadership) (Disterer 2013), the senior management must come to terms with the business reality and prioritise commitment critical to the design, CS preparedness, policy formulation and investment for any successful CSRM implementation practice (Chatterjee 2019; Zammani and Razali 2016). Top management support in providing adequate financial and human resources provides a solid foundation for CSRM implementation success. The resources include the purchase, operations and maintenance costs of assets, training costs for the CSRM team, auditors and dedicated personnel involved in CSRM activities and the cost of performing awareness and training programmes for employees.

The planning, implementation, monitoring and execution phases of CSRM require top management support to be feasible (Atoum, Otoom and Abu Ali 2014; Maarop et al. 2015). All these make CSRM implementation a discipline that mitigates business risks through top management's understanding, commitment, and support to make adequate security and business decisions that drive technical and operational success. Inadequate and wrong modalities of implementation and integration of CSRM practices into the strategic organisational practices result in failure crises (Lalonde and Boiral 2012; Leitch 2010).

- **Awareness**

Awareness in this study context means all stakeholders create a shift in thinking through supporting materials, guidance and training dedicated to inspiring positive behavioural,

attitudinal, and cultural change towards successful CSRM implementation. Cyber/information security literature and the international standards emphasize the need for a top-bottom or vice-versa awareness education and training for all organisation members as the 'gold standard' more than technical administration for CSRM implementation success (Merete Hagen, Albrechtsen and Hovden 2008; Shackelford 2016).

Effective CSRM is directly related to the awareness of increasing vulnerabilities, such as cyber threats and information warfare (Brauner et al. 2019; Haapamäki and Sihvonen 2019; Hussain and Skinner 2019). Most employees are naïve of CSRM expectations and the variables they must manage. However, the root causes of security and implementation problems are identified and explicit when issues arise (Ani, He and Tiwari.

The characteristics of role model organisations of now and the nearest future will promote consistent and effective CS awareness education initiatives and programmes to all employees via various mediums. This countermeasure manages CS implementation challenges, communicates CSRM goals and stops the probability of ill-motivated internal security incidents that have emerged from the general perception of technological and computer failures to multiple failures in people (Hadlington 2017; Torres et al. 2006).

Security awareness helps people recognise CS risks and threats and respond appropriately to mitigate them as an arsenal. The medium of awareness means communicating the necessary information, skills, and knowledge to stakeholders such as fliers, bulletin, electronic medium, verbal and much more (Tu and Yuang 2014). Users must be aware and vigilant to know the limitations of technology and exercise utmost caution to preserve the security environment through their behaviours.

- **Training**

Training is a formal learning process focusing on acquiring the necessary physical skills and competencies to perform CSRM tasks, processes, and procedures with minimal effort to achieve CSRM goals and business objectives. NIST SP 800:16 defines training 'as a level of learning that strives to produce relevant and needed security skills and competencies by practitioners of functional specialities other than IT security.'

Empirical evidence emphasised that CSRM implementation would need continuous and ongoing awareness and training programmes for employees to deal with the dynamic security field (Puhakainen and Siponen 2010; Kennedy 2016). Adequate knowledge and awareness training towards technology and its functions and the various security threats and countermeasures make people central to the implementation process and form top success factors in most studies. Failure in people through user negligence constitutes a more significant challenge to any CSRM implementation process (Ani, He and Tiwari 2019; Safa et al. 2015).

Security awareness and training aim to change employee behaviour and attitudes towards security culture and CSRM implementation importance and requirements (Ani, He and Tiwari 2019; Hadlington 2017). Often, improper employee behaviours towards organisation safety (CSRM implementation success) result from misunderstandings due to lack of awareness and training, culminating in inappropriate reasoning (Kraemer, Carayon and Clem 2009). Over time, continuous awareness and training gained by users and CS professionals enable CS competency development, alignment, and consistent successful implementation of security controls (Von Solms and Van Niekerk 2013).

Awareness and training act as a catalyst to CSRM implementation success. A practical training method about CS risks and its management move employees/stakeholders from ‘unconscious incompetence ‘ to a state of ‘conscious competence’ in their security activities and practices to become an invaluable part of de facto security behaviour and overall organisation’s CSRM implementation strategy. Employees' compliance with CS policies and performance is achieved through CS training (Puhakainen and Siponen 2010). Thus, the best CSRM investment is better training (Disparte and Furlow 2017).

2.7.3 Technology Factors

Technology will be significant in CSRM implementation success because organisations progressively use technology for business and social transactions. Technology/ ICT has made engaging in cyberspace immense importance for large organisations and digitised society. Technology provides the tools and resources to accomplish work activities (tasks) through processes (Troyer 2017). The hyper-connectivity in cyberspace exacerbates the complexity of the CS risks of participating in such a domain. The threats, uncertainties and vulnerabilities of cybercrime attacks continuously become more problematic and sophisticated, transforming into more advanced, more damaging, and unquantifiable menace (Neghina and scarlet 2012).

The technology dimension is a success characteristic and success factor in information systems and CS literature (Masike Malatji, Sune Von Solms and Marnewick 2019; Petter, DeLone and McLean 2013). Task-technology fit constitutes an important construct in security success (Petter, DeLone and McLean 2013). Realising that CS risk is becoming more sophisticated and seems inevitable in business, in-depth knowledge of information systems and risk management is vital (Hoffmann, Kiedrowicz and Stanik 2016; Webb et al. 2014).

In this study, the technology factor refers to the CSRM work activities to accomplish and the technology that aids its success. Technology factors include proactive and reactive measures comprising tools, techniques and resources (hardware and software, tangible and intangible) used to accomplish CSRM work activities (Kumar et al. 2020). Various technical solutions have been developed for CSRM, particularly with the information security of the TRIAD and more are still unfolding. While IT/ICT infrastructures hold much promise for enabling business process integration and mitigating CS risks, difficulties in availability, appropriate use, and implementation capabilities may lead to significant failures and inability to achieve the promised benefits (Dunkerley and Tejay 2011; Masike Malatji, Sune Von Solms and Marnewick 2019; Usman and Shah 2013).

The successful outcome of information security risk management has been attributed to the link between user participation in information systems security risks, control and system quality (Spears and Barki 2010). However, system quality as a measure of technology and a success factor of IS success and other related studies have been marred with mixed feelings (Petter, DeLone and McLean 2008; Petter, DeLone and McLean 2013). Nevertheless, the quality dimension of a state-of-art- technology in CSRM with best practice reflects the great potential of net benefit. Evaluation of system quality is an exercise of failure avoidance and success repetition in future rather than fault-finding (Palvia, Sharma and Conrath 2001).

In an e-commerce environment, Bharati and Chaudhary (2006) found a significant relationship between system quality and decision making satisfaction measured by reliability, ease of use, flexibility and convenience of use. Also, the availability of information technology systems is an indicator that allows organisations to evaluate the degree of alignment between the ability to adapt to changing and challenging risk environments and protecting the organisation's core assets and processes and business objectives (Torres et al. 2006). State-of-art technology has been at the heart of CSRM in recent times. Therefore, the reliability and availability of technology as a system quality measure is worthy of examination.

Various CS and IT studies propose that if information systems have been successful as a product, it is worth systematically documenting their success factors for replicating future CSRM/IS projects (Palvia, Sharma and Conrath 2001). Instead, rather than going over the old ground technical system, take the advantage to focus on people and processes. Having intelligent, competent, and honest system professionals will ensure a better alignment of security practices and efficient use of technology improvements and solutions. Hence, IT professionals, business and line managers share IT management to provide value as an impetus for successful CSRM practices (Perez 2013).

Cyber security risk management with IT products is a world of fantasy without the enrichment of IT competencies for better alignment between business, information technology and security objectives (Mitnick and Simon 2011) and the implementation of appropriate controls (Bendovschi 2015). Measures chosen for understanding the characteristics of the technology used for CSRM tasks from related research papers were adapted and grouped into variables that would represent: IT competence (Chang 2006; Pavlou and El Sawy 2006; Tu et al. 2018) and System quality (Bharati and Chaudhary 2006). These factors contribute to making the technology fit for performing the CSRM task, as shown in Figure 2.5.

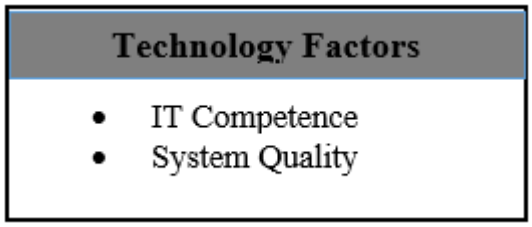

Figure 2.5: Technology Factors

- **IT Competence**

Kayworth and Whitten (2010) stressed the need for a balance between technical and social factors. IT competence is defined as IT-related direct and implied knowledge that a business manager possesses and exhibits (Bassellier, Reich and Benbasat 2001). Therefore, the successful implementation of CSRM is enhanced by the business managers and IT professionals IT skills and competence to drive CSRM implementation controls and practices. Competent IT staffs with expert skills are intangible resources that operate the IT resources. Such IT competencies increase IT capabilities to deploy and apply information technologies in the CSRM controls development

and implementation processes (Chang, Chen and Chen 2011).

Information technologies and competent IT staff support security control, such as policies and operational controls (backup and access controls) (Tu and Yuan 2014) for CSRM implementation success. IT competence would enable an organisation to devise a new way of thinking to plan, organise, implement, and invest in CS efficiently. Technological competencies consist of knowledge and new skills implanted in people and intangibles encapsulated in technical systems to deliver CS services. Strategic and operations integrations occur when the IT resources and competencies can support CSRM implementation processes and the business objectives (Rivard, Raymond and Verreault 2006).

This study conceptualised IT competence as the combined people's knowledge/skills and complementary capabilities of information technology resources to support the organisation's strategic competencies through the effective use and management of IT to consistently fulfil its CSRM objective, implementation success and competitive advantage. Therefore, this study's IT competence factors are derived and adapted from (Chang, Chen and Chen 2011; Tu and Yuan 2014) by interwoven relationships between IT staff, IT resources and CSRM operations.

IT competencies include IT resources and operations in an organisation that form the technical foundation of CSRM and competitive advantage in a digitized business environment (Pavlou and El Sawy 2006; Tu et al. 2018; Tu and Yuan 2014). IT competence construct was measured by how the end-users use IT resources and follow sound CSRM operations processes and how the IT expertise of staff (outsourced and inbound) has contributed to CSRM implementation success.

- **System Quality**

System quality has been studied as a dependent and independent variable of Information Systems Success (Petter, DeLone and McLean 2013). System Quality exemplifies one of the six measures of information systems success (Petter, DeLone and McLean 2013). System Quality considers the technical aspects of systems for use in CSRM and other risk management projects. Success variable measures, among others, include reliability, ease of access and navigation, system functionality, flexibility, and response time (Petter, DeLone and McLean 2013).

It appears that task compatibility as a measure of system quality regarding availability and reliability for CSRM implementation success is lacking in previous studies. Moreover, perceived

ease of use does not capture the system quality construct in totality (Petter, DeLone and McLean 2008). The central issue is that the taxonomy of most widely and robust studies on System Quality predictors are precisely the characteristics of the system's users' attitudes toward technology, self-efficacy, and technology experience, which can be easily influenced through training (Petter, DeLone and McLean 2013).

Petter, DeLone and McLean (2013) suggest further research to understand better the relationship or lack of connection between system quality as a success factor for the individual user. Moreover, few studies at the organisational levels have examined the relationship between system quality and user satisfaction (Petter, DeLone and McLean 2008). Emerging support and propositions among practitioners and researchers consider evaluation and quality are closely linked (Palvia, Sharma and Conrath 2001). The implementation evaluation of information systems should be seen as a quality assessment activity (Palvia, Sharma and Conrath 2001).

In this study, system quality is a multi-dimensional concept representing the socio-technical perspective concerning characteristics of the task, people, technology and organisation as the availability and reliability of the technology used to perform CSRM implementation processes and tasks (Palvia, Sharma and Conrath 2001). Choosing and implementing a suitable technology that provides a close fit between people, organisations, and processes is paramount for CSRM implementation success (Palvia, Sharma and Conrath 2001). CSRM implementation in organisations requires specific indispensable applications, operating systems, and other technologies (Kouns and Minoli 2011). The relevance and assessment of these qualities and attributes will vary considerably depending on different stakeholders, as exemplified in previous IS interpretive research (Orlikowski 1992; Orlikowski and Gash 1994).

Organisations lacking appropriate technology, tools, techniques, and resources required to enforce and monitor CSRM implementation will experience security issues. Such functionalities include suitable user interfaces, response time and system reliability. CSRM technical controls such as authentication systems, encryption and intrusion techniques, antivirus software, firewalls and many more are critical success factors for CSRM implementation in organisations, especially for fraud prevention in banks (Usman and Shah 2013). One might ask: are CS issues outperforming technology?

The quality of the technology systems used for performing risk management tasks in terms of their reliability, suitability, compliance with industry standards, and ability to cover all aspects of

the organisation's CSRM implementation tasks were important in this study. System quality as a success factor for this study is adapted in consistence with system quality measures in previous studies in many ways, including:

1) The fitness of the tools and technology for performing the CSRM implementation task regarding the availability of tools and their suitability for implementing risk management tasks (Lyytinen, Mathiassen and Ropponen 1996; Lyytinen and Newman 2008; Wang, Klein and Jiang 2006). Available and reliable tools and technology covering all aspects of risk management will improve the use of technology for CSRM. Standardized tools and technology used for CSRM enhance technology use for CSRM implementation success.
2) The technology's capability is used for CSRM within the organisation structure regarding the availability of knowledge bases to support the CSRM implementation tasks (Rivard, Raymond and Verreault 2006). Availability of knowledge bases improves the use of technology for CSRM implementation success. This helps the earlier assertions that users, technologists, managers' responses towards technology will differ based on job roles, needs and previous assimilation in their career and business environment (Palvia, Sharma and Conrath 2001).

2.7.4 Process Factors

The process dimension represents various risk management tasks of identifying CS risks, executing quantitative analysis and qualitative analysis, formulating and communicating risk responses, monitoring, and controlling CS risks, as defined in CSRM frameworks and standards. Security is a process, not a product (Mitnick and Simon 2011); the process involves understanding the real CS threats and risks and formulating the appropriate CS controls and incorporating countermeasures from the start (Scheiner 2002) in (Dzazali and Zolait 2012).

It is crucial to identify, implement and maintain the appropriate security controls to succeed in CSRM. Controls help decision-makers take predictive and corrective actions that influence organisational behaviours and facilitate CSRM implementation success (Atoum, Otoom and Abu Ali 2014). Organisations also need to empower the CS teams with the necessary tools, infrastructures, supporting mechanisms to perform their tasks properly. Process factors transcend subjective interpretation but locate their place in the frameworks and standards accepted by organisations and professionals worldwide. The National Institute of Standards and Technology

(NIST) categorises CS controls into three groups (SP800 30): (1) Technical controls, for example, antivirus software, firewalls, encryption techniques (2) Operational controls, such as operational deficiencies correction methods and enforcement mechanisms (backup capabilities, physical access controls); and (3) Management controls, which include non-technical controls such as usage policies and business continuity plans. The literature review identified CS controls that include implementing CS policies and practices such as risk management and standards application with a security audit to protect the organisation from CS risks.

- **Security Policies**

Large organisations use CS policies to establish CS in their culture (Goss 2017). CS standards also highlight the need to develop security policies to provide management direction and support for achieving its CS objectives (Mayer and De Smet 2017; Shackelford 2015). Organisational CSRM policies clarify the importance of CSRM to the organisation by defining the CSRM objectives and specifying the corresponding responsibilities of employees towards achieving the goals (Ma, Johnston and Pearson 2008).

Top management provides direction and support for CSRM through policies communicated throughout the organisation in a relevant, accessible and understandable form to employees (Disterer 2013). Well-developed CS policies recommend the employees' anticipated desirable behaviour and the sanctions as disciplinary measures to deter noncompliance (Osuagwu et al. 2015). CS policy awareness, education and training are mandatory to motivate employee support to a great extent towards the probability of success in the CS policy implementation process (Flowerday and Tuyikeze 2016; Siponen, Mahmood and Pahnila 2014).

Management creates these CS policies and must make employees aware, enforce and continuously maintain the policy relevant to business needs and effective CSRM implementation success (Al-Awadi and Renaud 2007; Okolo 2016). Examples of deterrents are policy statements and CS guidelines (administrative controls limiting system resource usage). In contrast, preventive controls are physical restraints to unauthorised users, such as password locks and 2FA (Dawson 2018).

A purposeful and operative CS policy and strategy well communicated by the management and understood by the employees will reduce the likelihood of successful cyber incidents (Osho and Onoja 2015). Next are the three typical process dimension sub-factors illustrated in figure 2.6.

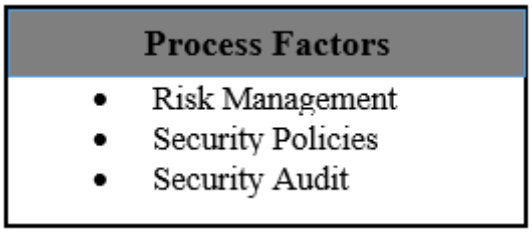

Figure 2.6: Process Factors

- **Risk Management**

The interest in the effects of risk management on CS continues to rise. CS now assumes an essential role as a new risk management dimension (Haapamäki and Sihvonen 2019). Risk management is the strategic management and mitigation of various CS risks by developing, implementing cost-effective countermeasures, monitoring, and reducing possible impacts of organisational CS risks to an acceptable level. The starting point for any organisation is the need to understand the risk triplets (threats, vulnerabilities, consequences) as well as the opportunities (risk analysis) that may affect the organisations' objectives and formulate risk management strategy to achieve adequate security (Dunkerley and Teejay 2011; Ganin et al. 2020).

Some literature reviews posit the effects of risk management on IT, MIS projects and information security risk management are hard to establish. Due to the extent and the difference in the risk management practices across different projects and their impact on project success dimensions. Recent studies suggest that the risk management practices are still at an embryonic stage and not widely used; only a limited number of organisations consider the socio-technical factors of these practices for their implementation success (Jean-Jules and Vicente 2020). Many have only used some, but not all, the available tools (de Bakker, Boonstra and Wortmann 2010; Kikwasi 2018). Hence, risk management applications in the CS domain need more awareness, training, tool development and research.

The risk management process is a vital component of a CSRM framework (Meszaros and Buchalcevova 2017). Risk management entails utilising appropriate steps or clear procedures to eliminate or reduce the organisational risk to a reasonable level (Kendrick 2010). Implementing a risk management approach supported with effective governance can help organisations manage cyber risks better while optimising their CS investments. The risk management process in CS

must create value, be cost-effective and not evolve with a reliance on universal measures that best protect information systems and best suites the organisation's CSRM implementation success.

The risk management process already discussed extensively in section 2.5 must be focused (ISO 2009) and aligned with the strategic, operational, and business objectives to improve the CSRM implementation process's performance. The risk management approach to CS is the best way to identify and implement the most helpful set of organisational CS controls (Hopkin 2017; Tisdale 2016; Tu and Yuan 2014).

- **Security Audit**

Researchers have studied the importance of CS audit as an integral part of CS and risk management functions across the entire organisation (Islam, Farah and Stafford 2018; Kahyaoglu and Caliyurt 2018). CS audit is an evolving dimension in security practice intended to support the successful implementation of security policies and processes to protect its critical security/information assets. The audit assesses the effectiveness of an organisation's ability to protect its critical assets (Onwubiko 2009).

Security audit in the CSRM framework has gone steps further from the usual financial, operational or management audits (Yang 2011). Security internal audit is a self-regulating assurance process that integrates risk management, security controls review and corporate governance to improve CSRM implementation operations and add value to the organisation (Yang 2011). Thus, security audit evaluates, supports the accomplishment of a cost-effective and quality financial reporting (Christ et al. 2015), control and improve governance processes (Ege 2015) towards successful CSRM implementation assurance process (Kahyaoglu and Caliyurt 2018). An internal security audit function helps achieve the needed structure and integration to achieve organisational CS goals (Kayworth and Whitten 2010). Internal security audits avert material weakness disclosures and increase the effectiveness of internal control and compliance processes (Lin et al. 2011).

This study conceptualises Security Audit as a systematic process that seeks to obtain proof of organisational CS policies, processes, procedures, and efficacy in the CSRM implementation success. To ensure CSRM is well implemented and maintained, the weaknesses in the processes, procedures and controls can be identified through disciplined security audits at scheduled intervals with an accompanying report of findings (No and Vasarhelyi 2017).

An extensive literature review above successfully achieves **Research Objective 1:**

> *To review the success factors in CSRM literature and understand the area focusing on large organisations.*

Although CSRM success remains a topical issue, there has been some progress in its implementation. The thesis identified success factors and groupings in the literature across regions. It provided sufficient support to explore the success factors for CSRM implementation in Nigeria currently lacking in the next chapter in achieving the second research objective. The following section highlights the reasons and needs to examine further success factors for CSRM implementation in large organisations in Nigeria.

2.8 Critiques in Literature

Reflecting on the literature review highlighted in Tables 2.6, despite extensive literature concerning risk management, information security and cybersecurity, security is managed across regional differences, practices, and contexts specific. Cybersecurity risk management is an evolving topic that cuts across many disciplines and regions worldwide.
An extensive review of literature analysing success factors in CSRM and its related field highlighted the lack of in-depth research in CSRM implementation success which is not entirely focused on technology.

Various studies focus on information technology systems as a significant cause of cyber security risk, focusing on the information technology domain (Dubois et al. 2010; Saleh and Alfantookh 2011). Section 2.7 highlights a few academic research types on CSRM focusing on organisations in Nigeria (See Appendix E). Much academic research focuses on information security and information security risk management in other developing countries. These show that CSRM can vary from one study context to another depending on the organisation's need. Although these studies give an insight into the study, they cannot provide a holistic picture of success factors for CSRM in large organisations in Nigeria nor its CSRM implementation success. At best, they can offer success factors for security around the perimeter fencing of the Triad.

Moreover, these studies were conducted in both developing and developed nations. From this perspective, this study undertook to study in-depth the success factors for CSRM implementation in Nigeria despite the substantial CS challenges for businesses and the government. Some studies

generally focused on information security management and information security risk management (Al-Awadi and Renaud 2007; Tu and Yuan 2014, Zammani and Razali 2016). These studies are not sufficient in isolation for a successful CSRM implementation.

Recent researchers have highlighted the need for practice-based research within the information security risk management domain (Bergström, Lundgren and Ericson 2019). The CSRM research literature typically would relate to other security aspects of the Triad. Research on information security risk management at the organisational level is essential (Kayworth and Whitten 2010; Shamala et al. 2017). Nevertheless, it fails to offer a balanced overview of CSRM implementation success, incorporating technical and non-technological factors. This is something of a pitfall. Social factors comprising behavioural and organisational factors avoid imbalance in CSRM solutions and complement CSRM implementation within an organisation (Jean-Jules and Vicente 2020; Kayworth and Whitten 2010).

Despite the need, effectiveness, and benefits of CSRM implementation, several researchers state that the organisations that have successfully implemented CSRM are few who do not exceed 20% by the most optimistic reports (Aminu 2013; Yaraghi and Langhe 2011). Therefore, CSRM requires balancing the social and technical factors to reduce the identified CS risks level to acceptable CS risk levels as the risks unfold (MCEvoy and Kowalsky 2019). Limited study explores cybersecurity strategies for preventing cyber exploitations in organisations in Nigeria (Alawonde 2020) in advancing similar research of five small industries in the USA (Saber 2016) in a multiple case study using thematic analysis. Shah, Jones and Choudrie (2019) highlight promising organisational practices for cybercrime prevention.

However, attackers are becoming more innovative in fraudulent gainful employment in their coveted targets (large organisations, including banks and customers), representing the largest adopters of internet revolutions (Wang, Nnaji and Jung 2020). It becomes a burden to organisations, government agencies, regulators, customers, and researchers for CSRM implementation to be successful, at least to a great extent. This thesis identified a lack of studies on the capability and practices of CSRM in these organisations and the knowledge in identifying success factors for CSRM implementation at the organisational level in Nigeria.

Likewise, there is a need for practice-based research that is flexible and allows participants to express themselves, complement and contribute to study in a meaningful way. The research will understand how these factors are implemented and evaluate how these factors influence CSRM

implementation success within large organisations in Nigeria. The need to identify the success factors for CSRM implementation and how CSRM implementation is done in practice is necessary for further analysis. Thereby fulfilling **Research Objective 2:**

> *To identify and evaluate factors influencing CSRM implementation success in large organisations in Nigeria.*

A review of published studies on security risk management in developing countries reveals that success factors for implementing CSRM have remained an under-researched area of investigation (Ani, He and Tiwari 2019; Dzazali and Zolait 2012). To counter and mitigate the cyber-attacks and CS risks, organisations should consider a risk management based solution with several factors influencing CSRM success. Such should include the people factors relating to the users' behavioural intentions and knowledge towards security assets and CSRM processes. Technical factors comprise the security software and hardware equipment to manage risks to information and information systems assets within the organisations. Organisational factors include modifications to the governance structure and process factors relating to CSRM processes.

Very few opinion-based published studies review CSRM at the organisational level from different perspectives such as strategic policy development (Osho 2015), information security management processes (Chang, Chen and Chen 2011; Ma, Johnston and Pearson 2008; Niemimaa and Niemimaa 2017; Thomson and von Solms 2006). These studies treat each success factor as a discrete independent factor and fail to consider specific latent inter-relationships between the factors. However, this study remains one of the few studies aimed at a holistic investigation of practitioners' perceptions concerning the success factors for implementing CSRM in large organisations in Nigeria.

Lastly, assuming absolving these studies of the above limitations, one could still argue that CSRM is a global concern. A continuous evolving process of balance of success factors for the prevention, detection, and response to risk management activities across technical and non-technical capability must be in place to mitigate CS risks as they appear. Therefore, the results cannot be transferred directly to this study context. This study proposes that investigating success factors for CSRM implementation is a gap in the literature and demand further attention due to the following reasons:

- Some of the previous approaches have mainly focused on information security management and information security risk management, which loosely or sparsely address the success factors for CSRM implementation. Information security management alone cannot protect or achieve the desired level of success in an organisation without an acceptable management policy and implementation (Von Solms and Van Niekerk 2013). Therefore, the studies could best strengthen a prevailing perception that CSRM implementation success is information security risk management implementation success. Hence, the CSRM context is still not widely understood.
- Success factors for CSRM implementation demand new thinking towards the assets to be managed beyond the fundamental technology factors for processes (Chabinsky 2014; Soomro, Shah and Ahmed 2016). Thus, humans are a core part of all social support networks as assets, threats, and vulnerabilities (Hadlington 2017; Ani, He and Tiwari 2019). To effectively manage the implementation of CSRM, there is the need to address the socio-technical aspects of CSRM of the entire organisation using a holistic view of their success factors. Therefore, the concept of factors that impact CSRM implementation success is still evolutionary and needs further investigation. Notably, the risks associated with ICT, information security, process, and human need significant consideration (Atoum, Otoom and Abu Ali 2014; Bednar and Welch 2019).
- Human risk factors are challenging to understand and mitigate. In most studies, practitioners lack a way to evaluate the reliability of the generic risk management perceived success factors in other related contexts as it applies to CSRM implementation success. Hence, rigorous qualitative empirical studies are necessary to validate and refine these factors in natural settings. This is necessary because CSRM is not a linear but a complex process with non-substantive, qualitative elements as factors to enhance its implementation success (Tisdale 2016). Quantitative methods seem inaccurate in CSRM because quantitative methods do not apply when human agents' acts are unpredictable (Hubbard and Seiersen 2016).
- Investigating success factors influencing CSRM implementation in large organisations in Nigeria is an overlooked study area in large organisations, almost in developing countries (Reza Hosseini et al. 2016; Usman and Shah 2013). Investigating large organisations' practitioners' perceptions concerning success factors for implementing CSRM in developing countries like Nigeria lacks investigation.
- Compared to the literature on ISRM implementation and practice, the research exploring the success of CSRM implementation practice in Nigeria has been scarce partly because of the topic's sensitivity; organisations are unwilling to discuss CSRM practice freely.

> Research investigating factors that influence CSRM implementation success requires researchers with in-depth knowledge of CS and risk management. Again, from the literature review, CS risks are not limited to one organisation or geographic location. Therefore, organising and supervising CSRM implementation activities may require inputs from several factors and stakeholders.

To further address objective 2, the literature review identified some important factors that might be necessary for CSRM implementation success from empirical studies, which were further grouped into four different dimensions as shown in Table 2.5, giving room for further analysis. Hence the research questions in section 1.6 study how these factors contribute to CSRM implementation success at the organisational level in a holistic view. Further studies of these factors provide answers for success factors for the CSRM implementation gap identified within this chapter.

Furthermore, the literature review identified a lack of theoretical models for success factors influencing CSRM implementation in a large organisation. For these reasons, case studies and developmental research that identify and evaluate technology and humans' influence on each other and arrive at the heart of complex relationships that often result in the continuous rise and decay of constant CSRM implementation practices is necessary. Perhaps, one can compare and learn how various organisations manage CS risks to inform better practice. In this regard, in chapter 3, a model of success factors that forms the conceptual framework to visualise how these success factors influence CSRM implementation was created (Figure 3.1) based on the various factor groups and elements derived from the literature (Figure 2.2).
Thereby fulfilling **Research Objective 3:**

> *To develop and propose a model for success factors for CSRM implementation in large organisations.*

The traditional dominance of CS/information security management research by mathematical or technological approach while the socio and organisational norms are taken for granted is no longer the case (Alawonde 2020; Coles-Kemp 2010; Fujs, Mihelič and Vrhovec 2019; Saber 2016). The organisational level CSRM implementation success is under-researched and attracts considerable interest in security. The socio-technical nature of CSRM and the human dimension to both CSRM implementation practices and technology designs must be recognised to manage these CS

challenges of today successfully. The organisational and social aspects must be part of the proper holistic study. Addressing these needs has been the motivation behind the present research.

Advancing previous studies when organisations worldwide face CS attacks become more critical than ever, especially in large businesses in Nigeria, benefit CS managers in other companies and sectors. As a result, exploring factors that influence CSRM implementation in Nigeria could prove vital in the research necessary for supporting the CSRM implementation success of organisations. Chapters 4, 5, 6 and 7 of this thesis answer and discuss the empirical studies implemented to address the research objectives. Thereby fulfilling **Research objective 4:**

> *To validate and evaluate the model within the practical arena and develop a novel contribution to the domain of large organisations and CSRM implementation.*

2.9 Conclusion

Dalal et al. (2021) elucidate the abundant, remarkable opportunities open to cybersecurity research and organisation interface. The current chapter reviews the literature to identify research problems in the area of large organisations. As a result, this study identifies literature gaps regarding the lack of theoretical models for success factors influencing CSRM implementation in Nigeria's large organisations. The reason is that CSRM is a relatively evolving area, especially in large organisations in Nigeria. Although few information security/risk management models exist, research studies on factors influencing CSRM implementation success in large organisations are few in Nigeria. However, this study conjectures that these studies may seem relevant, but concerns call to question their validity and applicability in large organisations in Nigeria. According to the literature review, the reasons are the distinctive characteristics of Nigeria, working practices and ethics, personnel and cultural differences and issues, and the factors change from one country to the other. Large organisations have more CSRM activities and processes than SMEs and other public organisations.

Also, in the light of the topic's sensitivity, known and recent events of alarming CS risks and challenges in Nigeria, organisations may be unwilling. This research study proposes that exploring CSRM implementation success in large organisations in Nigeria is a research gap with this evidence theorised in the literature. There is a lack of success factors for CSRM implementation models in large organisations in Nigeria. This issue could be a starting point for a model for evaluating success factors for implementing CSRM with a systemic view

incorporating social and technological perspectives as CS risks unfold in large organisations in Nigeria.

The chapter commences by reviewing the literature on CS and risk management. This study discusses the relevance of risk management in CS. For this purpose, this study conceptualises CSRM and establish a timeline that focuses on identifying the success factors for CSRM in large organisations in section 2.6. The review of success factors in large organisations in section 2.7 epitomises multiple factors, i.e., several common and various other domain-specific factors (Table 2.6). The explanation presented in Sections 2.8 thus far supports these study findings and the research objectives. Hence, the literature review derives the main research objectives summarised in Table 2.6.

Table 2.6: Highlighting the Research Objectives

Research Objectives for Further Investigation	
Research Objectives	**Description**
Success Factors Influencing CSRM Implementation	Lack of success factors influencing CSRM implementation in large organisations in Nigeria.
Success Factors Influencing CSRM Implementation model	Lack of success factors influencing CSRM implementation model in large organisations.

Chapter 3 considers and addresses the research objectives. It also discusses the conceptual framework and the theory that underpins this research.

Chapter 3: Research Framework

3.1 Introduction

The previous chapter highlighted some research problems for further investigation. The key research problems derived from Chapter 2 emphasised: (a) a lack of success factors influencing CSRM implementation in large organisations in Nigeria. (b) limited theoretical models that describe success factors that influence CSRM implementation in Nigeria. Hence, a relative gap exists for evaluating factors that influence CSRM implementation in Nigeria. (c) large organisations relatively have more CSRM activities and processes different from the private and public sectors. Therefore, have a different organisational structure, CSRM culture and decision-making process compared to other industries. Thus, large organisations' likelihood focuses on various factors that impact the decision to implement CSRM. This study uses a critical literature analysis reported in Chapter 2 to further analyse the area under study. Thus, to further investigate these research problems, this chapter aims to develop a conceptual model for success factors influencing CSRM implementation in large organisations in Nigeria.

Section 3.2 focuses on the theory developed for this research. Section 3.2.1 describes the prominent theories identified in the previous section. This section assists in building an understanding of the application of the existing theories in previous studies. Section 3.2.1.1 and 3.2.1.2 discuss the prevailing two theories, their understanding, and their applications in this study. As reported in Section 2.8, literature illustrates that: (a) none of the previous studies on success factors attempted to investigate factors that influence CSRM implementation in large organisations in Nigeria. (b) lack of success factors influencing the CSRM implementation model in large organisations in Nigeria, indicating a gap in the literature. Therefore, on further investigating this lack of literature on the factors influencing CSRM implementation in large organisations in Nigeria and prioritising factors, Section 3.2.1.3 involves developing theory, highlighting the importance of Socio-Technical factors in CSRM implementation success. Section 3.2.1.4 links the chosen framework to the study.

The success factors from the literature that may assist in supporting studying success factors influencing CSRM implementation in large organisations in Nigeria make a novel contribution of proposed success factors influencing the CSRM implementation model at the conceptual level in Section 3.3. Section 3.4 highlights organisations' security implementation success measures adopted in the study. Chapter summary and conclusions in Section 3.5.

3.2 Theoretical Development

3.2.1 Concept of the Framework

Examining CSRM literature seems no one size fits all theoretical framework or theory for CSRM research or practice. There are various views on the use and relevance of frameworks. Walsham (1995) comprehensively discussed the role of theory in IS case studies. The theory is needed to promote previous studies' interpretation and chart the framework for future research. Theory guides the research to avoid bias in the study and helps focus on how to converse with the participants (Yin 2018).

There are growing concerns about focusing primarily on critical success factors or associated failure factors (section 2.7), incongruent with CSRM implementation's imperatives and organisational differences. Conversely, the CSRM implementation view rests on several relevant theories over different stages of the implementation processes or phases. This indicates that CSRM practices involve some frameworks emphasising strategic organisation management and processes. Other broader views of security fields recognise some external and internal factors that influence security practices.

Developing a theoretical framework that underpins research work is vital to creating the research design. Theoretical frameworks illustrate the critical problems of the topic under study (Oates 2005). Organising this study was based on a detailed guide by (Labaree 2020). This section delves deeper into understanding the socio-technical systems theory and its evolution from the systems theory. Further discussed are a few CS and risk management theory applications and Leavitt's Model of Socio-Technical Systems. Finally, develop connectivity between Socio-Technical Systems and CSRM Systems to analyse and evaluate success factors for CSRM implementation by treating it as a Socio-Technical System.

The research considered the following theories to evaluate the success factors for CSRM implementation:

1) Critical Success Factors
2) Socio-Technical Theory

3.2.1.1 Critical Success Factors

Critical Success Factor is described as key areas in which satisfactory results will ensure successful competitive performance for the organisation (Rockart 1979). Bullen and Rockart (1981) summarised and defined critical success factors in organisational strategic planning.
Various studies and sectors used the definition of critical success factors in section 2.7. Critical success factors are not without criticism because of the lack of agreement on critical factors among authors and organisations. Criticism remains on limitations imposed by 'critical success factors' as organisations exhibit a higher complexity level comprising interdependent socio-technical factors (Jackson 2007). Identifying what is critical may be subject to different interpretations by management and staff, leading to differences in the importance of each critical success factor in different organisational contexts (Zafar et al. 2011).

Organisations are complex social contexts operating in unstructured, dynamic turbulence of sophisticated cyber threats. Critical success factors may often shift over time as the environment and participant's perception of the context develops (Williams and Ramaprasad 1996). This study agrees with Williams and Ramaprasad and posits that classifying some factors as 'critical' may be a fallacy of hasty generalisation and grammatical artefact that might be problematic, leading to CSRM failures and less cyber-free organisation. Therefore, the CSFs would be social constructs and subjective (Williams and Ramaprasad 1996).

The notion of CSF could somewhat lead to confusion and misplaced priorities of factors that can negatively affect organisational success depending on the size and elimination of the seemingly less prioritised factors that could be detrimental to an organisation. The neglect of a non-obvious factor misses many essential factors from the socio-technical systems perspective that might create another risky CS environment. The search for ways to reduce this confusion directs a focus shift from a critical success factor approach to a broader context approach optimising social and technical factors in a complex organisational environment with constant inherent CSRM challenges.

Critics of critical success factors theory would argue that there can be little doubt that CSRM implementation success is a multidimensional concept and implementation success factors vary according to the organisation's perspectives. A clear indication of the misconceptions is the exhaustive review of information success measures (DeLone and McLean 2003). A suggestion is that there are no standard measures of success, and these success factors are also limited to IS

success. Although risk management methodologies, tools and techniques were developed (Ionita 2013) to increase CSRM success, human factors are nearly missing in current CS risk analysis and management (Ani, He and Tiwari 2019; Kraemer, Carayon and Clem 2009). Thus, the definition of CSRM implementation success is illusory.

Larsen and Myers in Fortune and White (2006) argue that the factor approach appears to interpret implementation as a static mechanism rather than a dynamic phenomenon and lacks the potential to have different significance levels at various implementation mechanism stages. The critical success factors approach does not provide enough foundation for a conceptual framework for evaluating factors for practices in CSRM implementation success (Palvia, Sharma and Conrath 2001). The call for a holistic approach that addresses the management of CS risks' social, economic, technical, cognitive, and cultural factors is unsurprising.

Yin (2018) further states that case study theories do not necessarily need to be the explicit formulation of a hypothesis or proposition but the form of a detailed and straightforward statement. This study states that a systematic socio-technical way moves an organisation towards safe implementation practice where attacks might not succeed. As discussed in sections 1.2 and 2.3, CS risks are socio-technical and successful CSRM implementation designs must depend on the balance between the two dimensions (Malatji, Marnewick and von Solms 2020).

The literature review helped identify a combination of success factors common in the studies and could be integrated as variables to explore and evaluate factors influencing CSRM implementation success. Hence, the call for excellence in practice through the sufficient balance of social and technical factors (Bednar, Welch and Milner 2016; Kayworth and Whitten 2010). Though in a different research context, these studies and many more have demonstrated this. This study proposes the meaningful advance of analysis issues from critical success factors to socio-technical approaches. It is necessary to set and explore the topic within the evolutionary context of socio-technical systems theory research to provide a helpful guide to explore and frame the argument.

3.2.1.2 Socio-Technical Systems Theory

Socio-technical systems theory has its core idea that any organisational system's design and performance can only be understood and improved if both ‘social’ and ‘technical’ aspects are combined and treated as interdependent parts of a complex system (Jackson 2007; Zoto et al.

2019). The socio-technical systems theory concept first appeared in Tavistock Institute in London in the 1950s as innovative practices. It emphasises the best ways to match the requirements of both the social intricacies and technical complexities at all levels in an organisation to accomplish essential functions (Baxter and Sommerville 2011; Wu, Straub and Liang 2015) with positive economic and human results (Charitoudi and Blyth 2013).

Success is a socio-technical phenomenon in every purposeful activity. The over-arching philosophy continues to evolve in practice both within and outside social sciences to embrace achieving the organisational goals by 'optimising' the technical and social systems, which form the foundation and cornerstone of the theory (Chen and Duvall 2014). The synergy (i.e., joint optimisation) between people using technology solutions to tasks through processes within a social structure (organisation) (Carayon et al. 2015).

System evaluations have multiple dimensions that reflect the tasks, people involved, the supporting technology and the organisation (Orlikowski and Baroudi 1991). Neglecting the complex negotiation (independence of each other but interaction) that goes on between the two (socio and technical) factors is risky (Kemp-Coles 2009). The absence of such discussion about the influence of organisational and socio factors contributes to the mechanistic way of managing and implementing CSRM (Spagnoletti and Resca 2008). Hence, the evolution in knowledge management thoughts of organisation theories from mechanical to organic management models, structures or a blend of both in the dynamics of cybersecurity (Sallos et al. 2019).

Socio-technical theory receives growing attention within cyber/information security studies. For example, the analysis of cybercrime and CS in Nigeria (Olayemi 2014), determining strategies for implementing information security (Alawonde 2020), preventing data breaches (Saber 2016) and understanding information systems success factors (Petter, DeLone and McLean 2013). Malatji, Sune Von Solms and Marnewick (2019) emphasise the equal importance and joint optimisation of the social, technical and environmental dimensions of information security and CS practices for optimal organisational security performance.

Risk management is a complex process that should not be confined to the technical aspects as recommended by the standards, guidelines, processes and tools, the human aspect of CSRM management in isolation, but the interaction between socio-technical factors (Lee and Green 2015). Organisations require a common framework with standard controls as a guideline to assess their existing CSRM programme or build one from scratch to adequately secure and monitor their

readiness to withstand a barrage of CS attacks (NIST 2014). NIST (2017) risk management framework emphasises an organisation-wide approach to risk, highlighting the decisive engagement of organisational resources at three levels: (1) organisation level, (2) mission/business process level and (3) information system level.

The various components of Leavitt's socio-technical model of four interacting components – structure, task, actor, and technology has been used in cyber risk management impact and assessment analyses and designing effective organisation (Charitoudi 2013). These components are transformed and translated into risk management elements: Structure from the management point of view represents the organisation and other institutional factors that facilitate effective coordination and communication within the surrounding in which CSRM is performed (Mintzberg 1993). Task denotes the complexities and uncertainties of various risk management processes of risk identification, quantitative and qualitative analysis, responses, monitoring and control as defined in risk management standards. Actors represent the capabilities and perceptions of all stakeholders involved in CSRM, including top and functional management, end-users involved in CSRM implementation. Technology refers to the risk management tools and techniques available and used within the organisation for performing CSRM tasks (inputs) into outputs (successful CSRM). These studies provide a good background on using the socio-technical system approach for understanding CSRM.

Socio-technical system theory is not without criticism of the failure to keep up with technology trends and organisational developments (Baxter and Sommeville 2011), misconceptions of what a system is and represents-misunderstanding and wrong application approaches (Liang and Xiao 2013; Musman and Turner 2018). These critics contrast a new socio-technical theory philosophy paradigm with a new ontology (systems as real-world entities) and epistemology. It consists of ideas that remained unchanged with specific applications and general principles evolving to reflect the changing nature of technology and work practices (Davis et al. 2014).

Needless engaging in the academic debate of the distinction between system safety attributed to large-scale organisations such as construction companies, where terrible failures of any of its systems result in chains of environmental, human, economic and public trust damages and organisational CS safety of a menace ravaging the whole world irrespective of the organisation or size (Carayon et al. 2015). The large organisations in Nigeria share a similar system thinking approach to cyber safety (Salim 2014; Young and Leveson 2014). CSRM implementation success is of utmost priority for organisation survival, public trust, national and worldwide cyber peace.

The socio-technical perspective is often seen as one of the foundational viewpoints contributing to the distinctive and intelligent cohesion axis— for the information systems discipline and coherently enlarge its frontiers (Bednar and Welch 2019). Socio-technical view advocates and promotes evaluating these social and technical components' functioning with practical experience feeding theoretical development holistically (Salmi and Mattelmäki 2019). Further studies recommended using the socio-technical view as pointers for consultants and executives as the appropriate basis for analysis purposes and intervention strategies for practical work results (Appelbaum 1997).

3.2.1.3 Theory and Framework Adopted for the Study

The literature review has highlighted several factors which have been prominent in the literature. These factors are helpful because they offer a better understanding of the complexities of the processes and the dynamics within the CSRM implementation lifecycle. Sufficient evidence from the literature enabled this study to recognise the most relevant success factors according to the building blocks of the foundational viewpoints for success factors perspective in CS discipline long–term vitality.

From the big picture extensively discussed above, the maturity of the CSRM field can be treated as a socio-technical system. The current research has identified that success is independent of a single factor but requires several factors. The problems created by growing cybercrime and CS challenges and different social, technological, political, and economic environments increased CS breaches for small and large organisations, especially in Nigeria.

The social sub-system represents humans who carry out assigned tasks and interact with technology in large organisations. The technical sub-system is highly dependent on technology in data transmission, cutting-edge communication links and appropriate information systems (hardware and software) for carrying out CSRM tasks for implementation success to remain viable and gain a competitive advantage. The purposeful sub-systems may be optimised by the strategic alignment of sub-units with matching activities and outputs to the organisational need (Davis et al. 2014).

More investment and emphasis on the technical aspect of the socio-technical system and its practices neglecting the social aspect or vice-versa will automatically transform to sub-optimal or unsuccessful implementation performance (Davis et al. 2014). These will increase unpredictable

relationships and negatively affect overall risk management performance (Foster 2018). Thus, the assumption that a socio-technical approach focuses on harnessing the human and technical success factors of organisational CSRM implementation work results from the joint optimisation between the two (Bednar and Welch 2019). A socio-technical gap or implementation failure exists where such joint optimisation is lacking in Figure 2.7.

This item has been removed due to 3rd Party Copyright. The unabridged version of the thesis can be found in the Lanchester Library, Coventry University.

Figure 2.7: Socio-Technical Gap (Source: Masike, Sune Von and Marnewick 2019)

Although the relationships between technology, people, organisation, and processes are more often complex, iterative, and hard to predict, the socio-technical approach's unique opportunity as a framework for analysis cannot be underestimated (Troyer 2017). The socio-technical approach's current interpretation focuses on one fully integrated view and not two distinct (social and technical) boundaries of evaluation. Its understanding of how an organisation functions and implements from the people-centred perspective. As well as recognising that organisations pursuing survival in turbulent CS risks management environments thrive as self–creating continuously in an open system exploiting appropriate technology to ensure that systems are designed and engaged optimally in pursuit of success.

The discussions of the two theories (critical success factors and socio-technical systems theory approach) depict that no theory is perfect. The socio-technical theory is preferred over critical success factors discussed above because it aligns with the study context and presents broad but straightforward functional grouping, suitably well-defined and anchored in the extant theory. It offers a practical method derived in the field, which combines qualitative research techniques with socio-technical and human factor analysis to understand CSRM implementation success.

This theory could well be labelled theory for understanding, emphasising showing others how to view the world in a certain way and bring about an altered sense of how things are or why they are (Gregor 2006).

This study believes that the application of joint optimisation concept of socio-technical system theory can address the gap found in literature, help analyse and emphasise the significance of interacting socio factors (people and organisation) and technical factors (tasks (processes/activities) and technology) for successful CSRM implementation in large Nigerian organisations. In agreement with the qualitative, interpretative information system research by bewski's (1992), different stakeholders develop different attitudes to CSRM implementation success. Obtaining inputs from other participants based on their experiences in their organisational environments will make a quality exploration of success factors for CSRM implementation in Nigeria (Charitoudi and Blyth 2013).

Socio-technical theory in this research takes the form of explanation in IS that fits the interpretivist paradigm primarily to lead researchers to adopt the valuable concept of an 'idea' to explain how and why some phenomena occur about the real world that is useful to explore the capability of an organisation (Orlikowski 1992). The theory is an end product, not leading to predictive theory, new and exciting to explain what was imperfectly understood beforehand. In this study, the heart of CSRM implementation success rests in the keen and effective multi-dimensional process management that closely aligns the social and technical factors in resolving the intellectual paradox in large organisations in Nigeria.

3.2.1.4 Linking CSRM to Socio-Technical Systems

Previous sections have highlighted the socio-technical theory and its strong foundation in literature. The theory has evolved as researchers have used it to design and analyse industry and practice. Davis et al. (2014) call for bravery in extending socio-technical thinking in societal challenges concerning security, resiliency, crime, demographic changes, sustainability, design and functioning of future cities, and many more. This study proposes that socio-technical thinking and practice offer value-laden potential through careful analysis and improved understanding in the CSRM domain by taking a cue from the above applications of socio-technical systems theory. It conceptualises socio-technical thinking in addressing the objectives of this study to identify and evaluate the success factors that influence CSRM implementation in large organisations in Nigeria by creating and modelling it as a socio-technical system.

Establishing the connection between the CSRM system and the socio-technical system is necessary to achieve the objectives. The choice of extending Leavitt's model for the development of a model for identifying and evaluating success factors for CSRM implementation in large organisations in Nigeria is as follows:

- Based on Leavitt's model, classifications portray simple, well defined, and huge factors grounded in the existing theory. Also, risk management systems, like other socio-technical systems, are open systems for effective CSRM implementation success. By considering organisations firstly as open systems then as socio-technical systems, the concepts of socio-technical systems theory must consider technical structures and work roles together as two systems that were both parts of one whole system (Robertson et al. 2015). Leavitt's model explains the model's mutual alignment of components (Lyytinen and Newman 2008).
- This research explores success factors that influence CSRM implementation in large organisations in Nigeria. Leavitt's model is for changes in the organisational system. To help large and other organisations in their decision making and serve as a guideline to understand the factors that must be present and how they can contribute to change efforts to achieve better CSRM implementation success for increased competitive advantage.
- Leavitt's model is generic to organisational design and has been widely employed by researchers in various applications, as detailed in section 3.2.1.3, due to its simplicity, applicability, and extensive use.
- CSRM implementation can be modelled as a system interacting with the subsystems. A system is a combination of interacting parts, such that the whole is more than the sum of the parts. This is true of CSRM implementation. CSRM implementation is composed of interrelated factors. The CSRM documents and managerial decisions on risks identification and assessments, the people performing CSRM tasks, the tools and techniques used for performing CSRM functions and the project organisation constitute the interrelated parts of the system.
- Large organisations are systems comprising two sub-systems. A system could be social, physical, symbolic, biological, or both. Technical subsystems consist of the CSRM implementation tasks and the technology to perform those tasks. The social subsystem consists of people performing the CSRM implementation tasks/processes and the organisation and its surroundings, which requires CSRM to function with applicable guidelines and standards.

- A distinguished characteristic transformation of a system is a change that preserves its uniqueness at any point in time. Strategy implementation, growth, risk management are continuous changes in an organisational system. Goal-directed behaviour characterises the changes observed in the state of the system.
- The feedback mechanism mediates between the goal and system behaviour. The feedback concept is necessary to understand how the CSRM implementation can lead to success. In CSRM implementation, risk identification, monitoring, controlling processes, security audit documents are equivalent to the feedback function.
- The constant flow of information and interactions within the system environment could be defined as the input and output of resources, knowledge, and efforts. Similarly, decisions and adequate budgets are inputs taken for risk management. These inputs are transformed by quantitative and qualitative analysis into a risk register as output and actionable decisions to be implemented to treat the risks.
- Information concerning the CSRM implementation process or evaluation of the performance of the process's outputs is fed back as an input into the system, perhaps leading to changes in the implementation process (transformation) and future implementation success (outputs).

3.3 The Conceptual Framework

A framework is a basic structure that provides the foundation and supporting context of what the research aims to achieve. A conceptual framework represents the constructs and factors analysed and describes any causal link among them. This research does not relate to any existing theoretical CSRM implementation success framework. The first step toward extending a conceptual framework for this study started with synthesising the literature (Section 2.7) on CS/risk management's success factors. The research model of information security risk management/IS success factors suggested by Petter, DeLone and McLean and CSRM standards and guidance help define the variables for exploring the success factors for the implementation of CSRM.

Moreover, the literature on the socio-technical approach/theory helps explain the reason behind CSRM implementation success. This study refuses to limit CSRM implementation to the successful performance of the formal processes of risk management planning, identification, analysis, response planning, monitoring and control in information security risk management but a holistic view of the organisation. This is because CS and information security are often used without much difference interchangeably (Öğüt, Raghunathan and Menon 2011) to help identify

success factors that might be useful as guides and a conceptual model for organisations for CSRM implementation success.

It is argued that a framework considering a holistic approach to exploring success factors for CSRM can help provide management solutions that improve CSRM implementation. As such, this study was bounded as (a) excellence in implementation of CSRM through socio-technical systems approach as interdisciplinary, cross-cutting other disciplines that relate to business functions (Charitoudi, Konstantinia 2013; Davis 2014), (b) CSRM implementation is influenced, enhanced and impacted by socio-technical factors (Bednar, Welch and Milner 2016), (c) responsible modelling of the interrelationship and dynamics of these factors at various points and time in an organisation's operations/processes and lifecycle as the concept uses a top-down approach as opposed to bottom-up approach (Organ 2012; Greenwood 2011).

The success factors model will provide a valuable guide for organisations planning to implement CSRM successfully. It is better to consider the Petter, DeLone and McLean IS success model developed from the Leavitts model to explore implementation success from different perspectives for this study. Also, information security is part of CS implementation. Thus, socio-technical theory thinking offers concepts that help understand success factors for implementing the CSRM work process in an organisation. It is an approach to explore CSRM implementation success that considers technical, social, and organisational factors and human factors. The socio-technical framework offers a powerful conceptual approach to comprehending the design and implementation of CSRM work systems involving humans, technology, and tasks within their natural organisational environment. It asks intelligent questions about CSRM implementation success and how large business stakeholders think about and deal with them.

The literature review results are decomposed and emphasised the need for a more effective model for success factors for CSRM implementation in large organisations. Therefore, the research framework should combine and adapt the models for factors influencing CSRM implementation success with the literature's suggestions associated with excellence in practices and success in IS, as shown in Figure 3.1. This conceptual framework presents the influential success factors that optimally may give far-reaching results when understood to interact with each other, but this is beyond the present study's focus.

As previously stated, the review did not merely adopt all the identified factors seen in literature but limited to those familiar across many pieces of literature and suggestions for further research. Consequently, to make it applicable to CSRM, there is less importance on previous information

quality and systems measures. The previous studies' dimensions are adopted, and the success dimensions are grouped into four factors: People, Technology, Process and Organisation. Consistent with the primary aim of the study to explore success factors influencing CSRM implementation in large organisations in Nigeria and as a guideline for the present study, this study has focused on the following research objectives:

1) Review the success factors in CSRM literature and understand the area focusing on large organisations.
2) Identify and evaluate the factors influencing CSRM implementation success in large organisations in Nigeria.
3) Develop and propose a success factors model for CSRM implementation in large organisations.
4) Validate and evaluate the model within the practical arena and develop a novel contribution to the domain of large organisations and CSRM implementation.

The proposed conceptual framework addresses the following overarching research question:

What success factors influence CSRM implementation in large organisations in Nigeria?

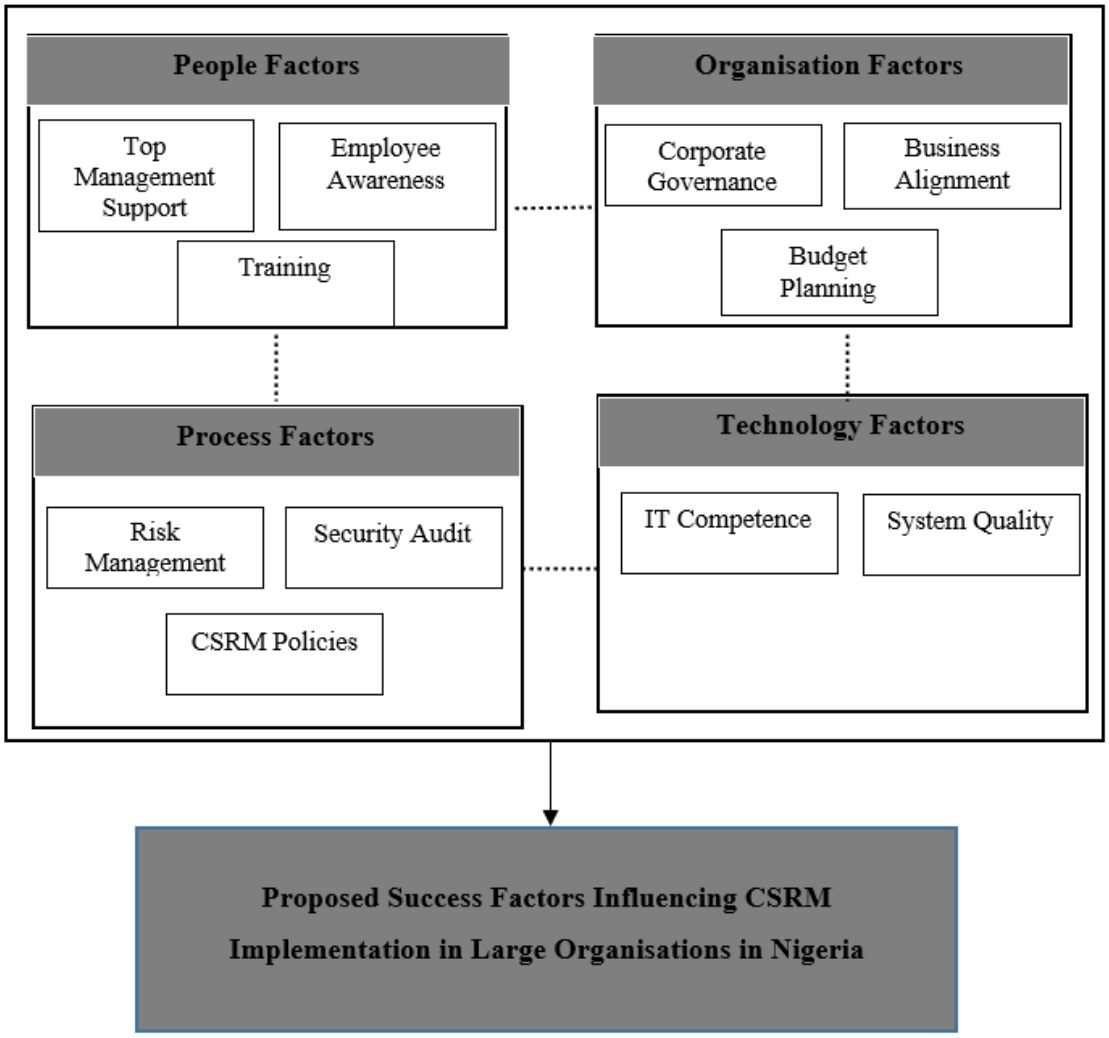

Figure 3.1: Proposed Success Factors Influencing CSRM Implementation in Large Organisation in Nigeria

Figure 3.1 depicts the proposed factors and make a novel contribution at a conceptual level. These factors are a combination of common factors identified from the previous studies on CSRM and other related fields reported in Sections 2.6.1, 2.6.2, 2.6.3, 2.6.4. This study extends these works and adapts them to success factors influencing CSRM implementation in large organisations in Nigeria. Nevertheless, these factors are yet to be evaluated in practice. Hence, this study suggests that the factors influence the successful implementation of CSRM in a large organisation in Nigeria and could provide a guideline for the CSRM implementation process. As a result, the proposed factors might: (a) extend the current research in success factors for CSRM implementation, (b) improve the level of success factors for CSRM implementation analysis and

(c) support the large organisation's decision-makers in CSRM implementation as a lasting strength of the varied, distinctive, yet integrated CSRM discipline.
Therefore, this study proposes the following research objectives for further investigation:

Research Objective 2- The proposed success factors (Figure 3.1) can influence CSRM in large organisations in Nigeria.
Research Objective 3- A success factors model can influence CSRM implementation in large organisations.
Research Objective 4- Validating and evaluating the model within the practical arena can develop a novel contribution to CSRM implementation and large organisations' domains.

According to the inductive approach taken to address the research questions and objective, statements corrected according to the inductive approach are more exploratory. This study's overarching research objective is to explore the factors influencing CSRM implementation success in large organisations in Nigeria. However, as stated in the study, a little bit of the evaluation aspect is necessary, noting that defining a specific measure was not the focus of this study. Hence, the efficiency/effectiveness and impacts measures can measure the success of the identified factors in evaluating and validating the CSRM implementation success in the organisations (Chew et al. 2008; Merete Hagen, Albrechtsen and Hovden 2008). More importantly, evaluate how organisations show successful improvements in CSRM implementations and what factors may influence these. Further details are covered later in chapters 5 and 6.

Successful operations depend on the social system's adaptive capabilities since the technical system cannot adjust nor adapt itself (Carcary et al. 2016). Focusing exclusively on technical factors/solutions– typical of engineers -haphazardly evolves and relegates CSRM implementation success to sheer good luck. It is hard to achieve successful performance, if ever, this way. This unavoidably leads managers to consider how people will associate with the organisation and organisational values and processes. The socio-technical systems concept of organisations as transforming organisations compels managers to view the organisation as a system and commit to a systemic CSRM implementation process.

When an organisation commits to implementing and supporting CSRM, the organisation often does so because of the expected positive organisational impact. Such include a high level of CSRM maturity against a CS breach's potential impact, damage to organisational assets (both

tangible and intangible assets), resilience to manage the fallout from the breach effectively and profitability (Petter, DeLone and McLean 2013). This study has adapted organisational impact as the effect of these factors on CSRM implementation success and its use on large organisations' performance in Nigeria. Therefore, continuously examine mutual interactions between technical and social components (factors) to achieve successful outcomes and the desired goals.

3.4 Conclusion

This study identified a gap in the literature that addressed the lack of theoretical models for success factors for CSRM implementation in large organisations in Nigeria. The literature review assisted in answering the main question partly:

What are the success factors for CSRM implementation?

Cyber security risk management is multifaceted and has been a topical issue in Nigeria. Some studies argued that Nigeria's risk management practices are weak, and CSRM is best at the infant stage. This resulted in a high rate of CS risks and threats in Nigeria. Eleven success factors for CSRM implementation were identified and grouped into Organisational, People, Process and Technological factors. The narrow view of socio-technological factors' complexities and their concealed impact on enhancing CSRM success complicates its implementation. A change in the CSRM paradigm necessitates enabling a factors-security-first approach at different organisational levels for successful CSRM implementation. These findings from the literature require the subsequent research questions to determine the success factors that influence CSRM implementation in large organisations in Nigeria:

1. What are the People factors associated with CSRM implementation success in large organisations in Nigeria?
2. What are the Technological factors associated with CSRM implementation success in large organisations in Nigeria?
3. What are the Process factors associated with CSRM implementation success in large organisations in Nigeria?
4. What are the Organisational factors associated with CSRM implementation success in large organisations in Nigeria?

A form of management that can exploit several theoretical approaches is at the heart of CSRM implementation success. The literature review provided valuable insights to fulfil the purpose of the study. By synthesising the most commonly used models and theories, namely, Delone and Meclane IS Success model, Critical success factor theory and socio-technical theory used in the literature, apply a relevant theory to accomplish the study objectives. The success of CSRM implementation in an organisation suggests an ecosystem related to the system theory approach (Jarjoui and Murimi 2021). Then, the advancement of Socio-Technical systems theory and its applications in several practice areas. Further developed the connection between the chosen Socio-Technical systems theory and the CSRM implementation system concept modelled as a socio-technical system about Leavitt's model.

A conceptual framework is not explicitly necessary in a qualitative study but not unusual. The initial conceptual framework outlined with the factors has a unifying theme described by a phrase or word to identify and evaluate factors that influence CSRM implementation success in large organisations in Nigeria is to guide the research and ensures consistency in the participants' response to questions (Yin 2018). The framework provides sufficient support to achieve the objectives to develop a conceptual success factors implementation model for CSRM.

Conceptual frameworks, however, need constant improvement between practice and theory (Lynham 2000). Hence, the framework's use did not intend to test theory; neither was statistical data used in the study. The next chapter details the need to formulate how the conceptual model is applied to CSRM implementation in Nigeria and the analytical tools and techniques used for analysing the result. The framework improves as studies reveal more relevant data and findings in tandem with this. The later chapters of this thesis cover the updates to this framework. While the proposed framework has started to address the main target area, there is the need to verify this in a further empirical study because of the topic’s evolving nature. This was accomplished during the later stages of the study, moving from theory to action. Table 3.1 summarises the proposed research objectives.

Table 3.1: Proposed Research Objectives for Further Investigation

Proposed Research Objectives for Further Investigation	
Research Objective	**Description**
CSRM implementation success factors	Factors proposed (figure 3.1) can influence CSRM implementation success in large organisations in Nigeria.
A model of CSRM implementation success factors	A model of proposed factors that influence CSRM implementation success in large organisations can be developed.

Chapter 4 presents the research methodology used to validate the proposed CSRM implementation success factors and research objectives proposed for further investigation.

Chapter 4: Research Methodology-A Qualitative Case Study

4.1 Introduction

Chapter 3 proposed and described the conceptual model for success factors influencing CSRM implementation in large organisations in Nigeria. Chapter 4 describes how this thesis 'research problem' will be resolved and achieve the research aim and objectives. Consequently, this chapter describes the research methodology used in this thesis. The overview revolves around the methodologies often adopted in the information systems field. Firstly, Sections 4.2, 4.2.1 and 4.2.2 review philosophical stances and lead to the intellectual justification of interpretivist as the research approach implemented in this thesis. Next, Section 4.3 discusses the choice of qualitative research in this study and further explains the differences between qualitative and quantitative research in Section 4.3.1, the benefits and limitations of qualitative research. Section 4.4 explains selecting the appropriate research strategy and the justification for the case study research strategy in Section 4.4.1. Justifications for the multiple case studies are highlighted in Section 4.4.1.1.

Furthermore, Section 4.5 presents the research methodology that serves as a guideline for undertaking an empirical inquiry. Section 4.5.1 presents the research design. In Section 4.5.2, 4.5.3, 4.5.4 and 4.5.5, the methodology translated into a protocol that serves as a data collection tool whereby data are deduced from case organisations in large organisations in Nigeria to resolve the proposed research objectives and validate the conceptual model. This research overcomes the risk of bias in literature when using the qualitative research method through data triangulation, as exemplified in Section 4.6. The case study protocols are presented in Section 4.7 and further provides details of the fieldwork process in Section 4.7.2. Section 4.7.2 addressed and presented the research objectives. Then, the description of the research outcome and presentation in section 4.7.4. Section 4.8 addressed the ethics and privacy issues, and finally, Section 4.9 summarises and concludes the chapter.

4.2 Selection of an Appropriate Research Philosophy

The research design process selects the best research philosophical approach for this study (Walsham 1995a). The research question depicts the characteristics of an ideal research question. The clarity, direction and focus require data collection, valuable and relevant, linked to and guided by relevant theory and previous research relevant to CSRM (Ritchie et al. 2013). It allows

generating findings that contribute to improved CSRM implementation success knowledge and practices. Section 3.2.1 explained that information/cybersecurity is a multi-disciplinary research area with many aspects of a specialised subject that is not grounded in a single theoretical perspective (Orlikowski and Baroudi 1991). Stafford Beer pointed out that "a theoretical framework is necessary for any empirical investigation; this is the raison d'etre of epistemology" (Maturana and Varela 2012:68). Thus, cyber security researchers access various philosophical assumptions about the underlying nature of the phenomenon under study. Each philosophical approach has its strengths and weaknesses (Galliers 1985).

4.2.1 Underlying Philosophical Assumptions

Research philosophy or research paradigm is a philosophical underpinning that guides this study in data collection procedures, data analysis techniques and interpretation (Mackenzie and Knipe 2006). Several research paradigms exist to gather information and control research conduct (Cohen and Cohen 2018). There is no fixed justification for the best methodology in any business and Information Systems domain research (Saunders et al. 2016).

Ontology denotes the set of beliefs about the nature of reality that exist in the world (Bryman 2015; Walliman 2017). Epistemology assumptions refer to how knowledge is understood and developed (O'Gorman and MacIntosh 2014). Questions inquire about the reliabilities of knowledge sources, what could be known and the truth's nature (Chilisa and Kawulich 2012). CSRM tends towards information security technical orientation, and researchers are frequently busy developing technical protocols and other matters. Communicating CSRM is confronted with paradoxes, which have resulted in various factors affecting the implementation success to deal with the risks and threats in large organisations, especially in Nigeria.

On this premise, this study focuses on examining the experiences of human actors concerning the factors influencing CSRM implementation success in large organisations in Nigeria (Ale, Aven and Jongejan 2009; Guba and Lincoln 1994). The intellectual reasoning and assumptions of this study are now explained. This study examines the various research philosophies available in CS/information security domain. Then, chose the research philosophy fit for answering the research questions to explore success factors that influence CSRM implementation in Nigeria.

- **Positivism Philosophy**

Positivism generally shares a philosophy similar to scientific methods that establish the future outcome by identifying and assessing a one-directional cause and effect (Creswell 2017; Saunders and Lewis 2017). The research results are grounded on the hypothesis formed and empirically tested to verify the truth of what exists in practice through surveys, close-ended questionnaires, and experiments (Bryman 2015; Creswell 2017; Walliman 2006). Orlikowski and Baroudi (1991) propose that IS can be categorised as positivist if there is proof of systematic propositions, quantifiable variable measurements, hypothesis tests and conclusions on the phenomenon from a sample perspective to the given population.

More of a quantitative approach believes that human qualities are within scientific understanding (Bryman 2015). Hence, its criticism that human experiences cannot be examined in depth (Crossan 2003). It does not correctly represent the social realm but the physical world detached from humans. The phenomenological philosophy of the social world of business and management transcends theorising by strict laws similar to physical sciences and would reveal the details of the situation to comprehend the reality, or perhaps a reality working behind them (Ritchie et al. 2013; Saunders et al. 2016).

This study intends to see how theory can be interpreted and combined to understand what exists in actual practice through participants' shared experiences in large Nigerian organisations. Therefore, adopting a positivist paradigm limits the gains of in-depth knowledge of the identified success factors from collaborations and interactions with research participants. Adopting the positivist philosophy for this study is unnecessary. The literature posits that effective response to many security challenges requires a different epistemology perspective relevant to IS research and a common positivism approach (Spagnoletti and Resca 2008; Coles-Kemp 2009). Understanding the organisational and the societal aspects that respond to CSRM implementation success needs to be examined and interpreted subjectively (Alawonde 2020; Saber 2016 and Walsham 1995b).

- **Interpretivism Philosophy**

Interpretive research derives its philosophical stance and principles from anthropology, phenomenology, and hermeneutics (Klein and Myers 1999). Interpretivist assumes that knowledge of a fact or reality is gained through social constructions wrapped in people’s world

perceptions (Creswell 2007; Mackenzie and Knipe 2006). IS researchers focus on interpretive research to understand people's actions and thoughts within the socio-organisational environment. Interpretivism research focuses on human sense involvement as the situation emerges; hence, it does not predefine independent and dependent variables (Kaplan and Maxwell 2005). Walsham (1995) understood the interpretive approach to qualitative research studies and noted that it is necessary to access existing theory in a specific area, thinking that it is an ultimate fact in this field is the erroneous blurring of ideas in this field ongoing space.

4.2.2 Choosing Interpretive Research Philosophy

Many social scientists have made a culture shift from a laws-and-instances perfect explanation towards a cases-and-interpretations from the analysis drawn from understanding humanities coming to play in social and technology contexts within the organisational environment (Geertz 2004). More than a decade ago, Walsham (1995), in a comprehensive study, justifies the importance of interpretivist case studies in IS research. The background knowledge, literature review and analysis presented in the first three chapters suggested the basis for classification and show that the socio-technical factors (organisational, people, process and technological) seem complicated and interrelated (Section 3.2.1.4). Hence, the idea of viewing the totality of 'organizational systems' proposes verbal models to explore experiences (Drack and Schwarz 2010).

The rationale for selecting the research method and study design was derived from the research questions, objectives, and requirements. The choice of interpretivist philosophy is to gain an in-depth understanding of the various success factors that influence the assimilation of human knowledge and practices of CSRM implementation in the different case organisations in Nigeria through collaboration and interaction with the staff (Miles et al. 1994). Interpretivist endorsed the truth through fieldwork (interviews), interacting with participants to obtain the realities of their human consciousness and subjective experiences to understand success factors for CSRM implementation in large organisations in Nigeria (Burrell and Morgan 2017).

The interpretivist paradigm acquires knowledge and understanding by interpreting results from field interaction with participants' actual experiences in their natural environment (Creswell and Creswell 2017). In implementing CSRM, many managers and employees are involved based on their tasks with a specific activity. These individuals have different perspectives and perceptions of success factors for CSRM. The appropriate strategy to gain knowledge on these success factors

on CSRM implementation is to understand and learn these various participants' perceptions in their natural setting, representing their social world.
Thus, the researcher neutrally collaborates with participants, understands their perspectives, views the context meaning and provides a holistic perspective. The analysis report in Chapters 1 and 2 indicates that the study of human actions and behaviour in large organisations is distinct from other sectors. There are irreducible minimums that are infinite and must be observed in their entirety; such is the universe and the human behaviours-the social world.

In summary, interpretivism aligns with this study. It stresses the importance of interpretation based on the interaction between the managers and the employees in gaining deep insights into factors that influence CSRM implementation success in the large organisations in Nigeria- the social world (Crotty 1998). The qualitative nature and the acquired knowledge characteristics are a value-laden research process, dynamic, socially constructed meaning from researcher reflexivity on the study of multiple subjective realities from people in their natural environment, data analysis with numerous interpretations (Scotland 2012).

4.3 Differences between Qualitative and Quantitative Methods

Qualitative research involves interpreting non-numerical data (Miles and Huberman 1994). It offers analytical methods for a thorough understanding of the meanings of soft data such as words and sentences (Neuman 2015). Qualitative research investigates what is believed to be a socially constructed empirical truth through a value-added, versatile, interpretive, holistic and context-sensitive framework (Yilmaz 2013). The research approach includes purposeful sampling, open-ended collection and evaluation of drawings and texts (Creswell and Creswell 2017). These definitions suggest that qualitative research involves the making meaning of an in-depth overview of a phenomenon from the viewpoint of the people engaged through sources of data collection, including observations, interviews, and questionnaires. Qualitative research is a cross-disciplinary approach across domains and topics (Denzin and Lincoln 2012).

Comparatively, objectivist epistemology drives the Quantitative approach and aims to establish universal expository rules in social behaviour by statistically measuring what it believes to be a static reality (Yilmaz 2013). It promotes the idea that social phenomena have an objective truth independent of the subject matters under investigation. It includes data collection, analysis, and interpretation by experimental and surveys (Creswell and Creswell 2017). The differences

between qualitative and quantitative research designs and their fundamental beliefs, goals, methods, and functions are summarised in Table 4.1.

Table 4.1: Differences between Qualitative and Quantitative Research Approaches *(Source: Halliday 2007)*

This item has been removed due to 3rd Party Copyright. The unabridged version of the thesis can be found in the Lanchester Library, Coventry University.

The two approaches, qualitative and quantitative, are not without criticism. The qualitative method is not without limitations of smaller samples and time-consuming during interviews. Conversely, ticking off boxes, low administrative cost and assigning numerical scores in quantitative survey method with lesser or no time answering descriptive questions allow data collection within a widely dispersed population with no geographic limitations within a short period. Although the result can be compared across the broader population, quantitative results are measurable and require rigorous statistical analysis. The quantitative method's major drawback is that it can suffer from a low response rate and inflexibility. The participants are often restricted to ticked boxes with somewhat incomplete understanding, assuming the generalised result as objective truth. In contrast, the purposively selected interviewees in qualitative research ensure some samples' diversity with tackling different key aspects of CSRM implementation. Based on the discussions, the justification of qualitative research for this study follows.

4.3.1 Justification for Qualitative Research Method

Choosing the appropriate method that achieves the objectives is vital by establishing the research objectives and examining theoretical contributions to the literature (Saunders and Lewis 2014). Yin (2009) defines the research method as the blueprint linking the research questions with the empirical data, findings, and conclusions. This study adopts a qualitative research method rather than a quantitative research method, common in recent organisational cybersecurity research (Fujs, Mihelič and Vrhovec 2019).

Firstly, this study chose the qualitative method because of the philosophical stance of this research. Qualitative research is informed by interpretivism position. Secondly, qualitative research characteristics, for example, handling social situations and unexpected emergent concepts, suit the subject of exploring the success factors for CSRM implementation in large organisations in Nigeria (Walliman 2017). In contrast, Quantitative research is linked to the positivist paradigm involving data gathering in numbers and statistical procedures of analyses (Halliday 2007). Quantitative research often validates or change a previously formulated hypothesis. Thus, the quantitative research method is inappropriate for the study; the qualitative research method has its place.

Qualitative research focuses on advancing data and ideas through careful interpretations of words' social meaning to provide a holistic understanding of research participants' actions and views (Walliman 2017). This qualitative study aims not to report statistical relationships among variables standard in quantitative studies but to explore and interpret the success factors for CSRM implementation. Thus, a qualitative methodology was suitable. The participants' ability to talk through their experiences at interview distinguish them from the world around them (Klein and Myers 1999). Evaluating participant experiences were essential in CSRM implementation success in improving systems protection from CS incidents and breaches.

No doubt, qualitative studies are explorative and useful in agreement with (Yin 2018). There is a need to investigate unique events or issues when exploring complex CSRM implementation success phenomena. Hence, qualitative methods to explore, examine and evaluate success factors for CSRM implementations prevent cyber exploitation. This motivated the adoption of a qualitative method as it allows for in-depth explanations, understanding and interpretations of several aspects surrounding the success factors for CSRM in the large organisations in the Nigeria context. Neuman (2014) agrees with a comprehensive qualitative analysis of success factors in

real case studies of large Nigerian organisations while implementing CSRM, typical of ‘cases and context’ from the principle of social sciences or interpretive research.

The epistemological view suggests that qualitative research is an appropriate approach. It encourages closer collaboration with the purposeful sample of participants with relevant experiences on success factors for CSRM implementation in the case organisations in Nigeria to get a proper understanding and the significance of their experiences instead of a particular set of techniques (Yilmaz 2013).

Thus, qualitative research's choice helped this study understand the socio-technical-organisational context. The interaction of the people involved in accomplishing the CSRM implementation and coordinating their work (social) and technical factors (the nature of the CSRM process to be performed and the technology to complete the CSRM process) creates the conditions for the successful CSRM implementation in large Nigerian organisations.

The detail of success factors for CSRM implementation is intellectually found in the process of interaction with a purposive sample size in the particular context of large organisations in Nigeria within which they operate (Silverman 2017:134). This is opposed to the quantitative study involving numerical data collection from structured surveys closed-ended questionnaires from a large sample size compared with qualitative research (Neuman 2014). Thus, the often use of statements such as ‘many or majority agreed’, ‘some argue’, or ‘it was frequently observed that’ by qualitative research, practitioners explicitly refer to a statistical distribution. Vague as they may seem from the beliefs of quantitative researchers’ mathematical points of view, they shed light on the topic under study.

The design of a qualitative research approach is to capture the reasoning in practice. A rich insight gained from a few samples of participants possessing requisite knowledge and expertise in case organisations helps understand success factors for CSRM implementation processes (Patton 2015; Silverman 2017). Therefore, statistical generalisations were not the priority of this study; instead, a saturation of the chosen topic identifies patterns in the answers, and themes reoccur.

Furthermore, since the present study, perhaps the first to examine the success factors of CSRM implementations in large organisations in the Nigerian context, this study perceived the qualitative research as more appropriate to meet any unexpected issues. The researcher’s reflectivity on the topic throughout the process of data collection provides a level of reliability

and the potential to explore innovative study, allowing the understanding of complex social phenomena such as success factors for CSRM implementations in the Nigerian context (Holloway and Biley 2011; Ritchie et al. 2013).

Success factors for CSRM implementation, the main theme of this research, are complex processes that require an adaptive and flexible research design. Indeed, any study that explores an implementation in general, particularly CSRM implementations, involves collecting rich data with a high response rate, better insights, and more convincing cases of the numerous and multidimensional aspects of the implementation. Qualitative research supports ideally investigating such matter as it provides in-depth understandings and interpretations of researched Nigerian environment in a more flexible way (Creswell and Creswell 2017; Myers 2009).

As further discussed in detail in the following subsections, this research involved case studies selected purposively. Qualitative research collects and handles very detailed data of success factors for CSRM implementation within the purposively chosen interviewees. IS studies welcome shaping their research in terms of its necessities instead of perceived ideas of what fits or ought not to be doing? Various other studies have used the qualitative approach in studying critical success factors (Al-Awadi and Renaud 2007; Fujs, Mihelič and Vrhovec 2019; Holloway and Biley 2011; Lund 2014; Webb et al. 2014; Zammani and Razali 2016), which were adopted and adapted better to suit the characteristics and the necessity of this study. The empirical work involves interviewing experienced CSRM practitioners to expand the identified success factors derived from the literature review (Myers 2013). The reflectivity systematically unpacks and promotes this research's value to the knowledge base (Ben-Ari and Enosh 2011).

Four case studies were conducted, suggesting that the ‘value-free’ and ‘one world’ positivistic quantitative research concepts would be unhelpful (Denzin and Lincoln 2011). Investigating the success factors of CSRM implementation involved a deeper understanding of the socio-technical factors categorised into four dimensions: Technology, Process, People and Organisation. The key players of CSRM implementation, their activities, the organisational support structure and the managerial decisions to ensure CSRM success constitute the people dimension (Werlinger, Hawkey and Beznosov 2009). The organisation's indicators reflect the responsibility and communication structure concerning CSRM instituted in the chosen case organisations in Nigeria.

Previous studies (Allen et al. 2018a; Trim and Lee 2014) indicate that the organisation's structure should allow for the inter-weaving of CS governance into its very fabric. The structure should

encourage collaboration between CS specialists and business managers; and that CS mission, goals and objectives align with the overall organisational mission, goals, and objective. The process dimension defines the CSRM's major activities and practices to be performed by the leading players. It also specifies the vital documents to be established and followed. These categories consist of sub-factors that enhance CSRM implementation success by looking for themes, patterns, ideas capable of qualitative methodology rather than testing or confirming the hypothesis (Collis and Hussey 2003)- Objectives 2 and 3.

The exact nature of qualitative research is considered helpful for this study to obtain rich information and in-depth understanding when exploring success factors involving human, technical, process and organisational phenomena in IS research (Klein and Myers 1999; Walsham 1995). The experiences of interview participants will be subjective and will be relatively difficult to measure. The quantitative research method cannot 'measure' some social phenomena created by people; the need for the qualitative study has its place to achieve relevant results.

In summary, qualitative research suits addressing the research aim and questions. This method can expose the impact of social and technical factors in different organisations and situations, such as the success of CSRM implementations. Failure to qualitatively analyse and evaluate the decisions around these factors that represent the 'Achilles heel' for an organisation will be inappropriate due to the following reasons:

- A study that involves less acknowledged phenomenon, i.e., success factors that influence CSRM implementation in large organisations in Nigeria.
- A study that evaluates in-depth problems and processes.
- Investigation for which related factors have to be identified and evaluated.
- A study that must allow flexibilities during interviews and observations.
- Research that cannot be carried out experimentally for ethical and practical reasons.
- The study success factors influencing CSRM implementation in four large case organisations' natural settings.

Furthermore, qualitative research allows investigating the possible effects of phenomena such as CSRM implementation success. These characteristics correspond with the chosen research philosophy. The qualitative method now selected, selecting a research approach, requires careful consideration of the investigation's intellectual preferences.

4.4 Selecting the Appropriate Research Strategy

One of the methodologies that guide research to answer the research questions is the research strategy (Saunders, Lewis, and Thornhill 2016). Research strategy links the data collection and analysis methods with the study (Sekaran and Bougie 2016). Case study, experiment, survey, and action research are strategies applicable to business and management studies (Creswell and Creswell 2017; Lee 2017; Yin 2014).

4.4.1 Justifying the Choice of Case Study Research

This study chooses a qualitative case study to seek the contextual meaning of a research problem within a complex and bounded system (Yin 2014). This study explores the success factors for CSRM implementation as multiple case studies in organisations as a bounded setting in this similar empirical context. Several writers in the IS field have already demonstrated that interpretive case studies can make a valuable contribution to both IS theory and practice if carried out and written up carefully. According to Neale, Thapa and Boyce (2006), a case study captures what occurred and may provide a better opportunity to outline success factors for CSRM implementation by presenting the result's story. Other studies have used case studies while investigating critical success factors perspectives in related fields (Bergeron and Begin 1989; Rockart 1980). More significantly, from an information security risk management perspective (Zammani and Razali 2016).

4.4.2 Multiple Case Study Research

Yin (2018) suggests that case studies are recommended and appropriate for this study, including social dimensions within intricate settings, requiring an in-depth understanding as explained in the previous sections. Information system and socio-science studies have advanced from quantitative (laws and instances) to more qualitative, case-interpretive studies (Yin 2018). The humanistic-validity case study methodology works on the same goals and shares the same goal of knowledge without quantification or test of significance (Yin 2018).

In this research, multiple case studies better suit the identified success factors from the literature review. The motivation for using theory in the earlier stages of interpretive case studies is to create an initial theoretical framework that considers previous knowledge, which forms a reasonable

theoretical basis to inform the early empirical work's topics and approach. Yin (1981) firmly dispels the stereotype that case studies are more suitable only for exploratory research stages. Lately, researchers have further pointed out a need and adopted multiple case studies research within the information/CS domain (Alawonde 2020; Saber 2016).

The relevance of case studies to this study are as follows: the necessity to seek and understand personal views of CSRM in large organisations in Nigeria; the need for insights into factors that are important in CSRM implementation success (Yin 2013). In agreement with Bryman (2015), the interviews lead to multiple realities. The case study's unique strength is its ability to deal with a full range of evidence such as interviews, artefacts, documents, and observations (Yin 2013) with data converging in a triangulating approach. In this study, the case study aligns with the chosen research methods, interpretive philosophy, and research design.

Case studies are more than just an expected 'story' but qualify as theorising the exercise to conclusions with some generalisation (Klein and Myers 1999). Similarly, this research adopts the case study as well-defined research approaches to empirically provide answers to the research question (s). The research begins with the socio-technical theory analysis, which focuses on the reviewed literature and sets the context to the conceptual framework design (Guba and Lincoln 1985). The analysis also helped develop a practical research design for collecting data (Yin 2013).

4.5 Empirical Research Methodology

The research wheel is a way of directing the research process phases (Rudestam and Newton 2014). The wheel metaphor suggests that research is not linear. Still, a recursive cycle of steps is repeated over time to validate the empirical stages with the theory from where the theoretical concepts stem. Creswell (2018) emphasised rigour is essential in qualitative research design. These procedures align with the complexity of the social setting under study.

Jankowicz (2013) advanced an empirical research methodology which aligns with the analysis of the literature that indicates the basis of this research methodology phases on the following three stages of the qualitative research design: (a) define and design (b) prepare and collect (c) analyse and conclude. Based on the research design, an empirical research methodology was developed, which acts as the blueprint for the research process to evaluate the proposed conceptual model (Figure 3.1) and the research questions (Table 3.1) related to success factors for CSRM implementation in large Nigerian organisations.

4.5.1 Research Design

There is no universal structure on how to design a qualitative study, but the subject evolves. All researchers seem to begin with a problem, review the literature related to the problem, ask questions, collect data, analyse it, and write a study (Creswell and Poth 2016). Analyzing the data relates to the strategic decisions on which type of research to conduct (Creswell and Poth 2016).

This research is a cross-disciplinary topic with some specific problems. The research design is set to address the research questions. The research method consists of three phases to develop a comprehensive conceptual model of success factors for CSRM implementation that addresses the research objectives. Case study design links the first and last phases of the research design's developmental diagram, as shown in (Figure 4.1). Yin, a prominent pioneer in case study approaches, stressed that case studies could help understand the presumed causal relationships among variables too complex for survey design (Yin 2009). The recognized leader explains that theoretical ideas are critical to case studies design and are usually developed before data collection as they influence the data collected (Yin 2009).

Yin (2014) methodological approach of multiple case studies comprising three stages was adapted and provided a design framework for conducting the case studies, description, and analysis (Figure 4.1). The stages are (a) define and design, (b) prepare and collect (c) analyse and conclude. The pragmatic research design evaluated the conceptual model developed in chapter 3 and the research questions related to CSRM implementation in large organisations.

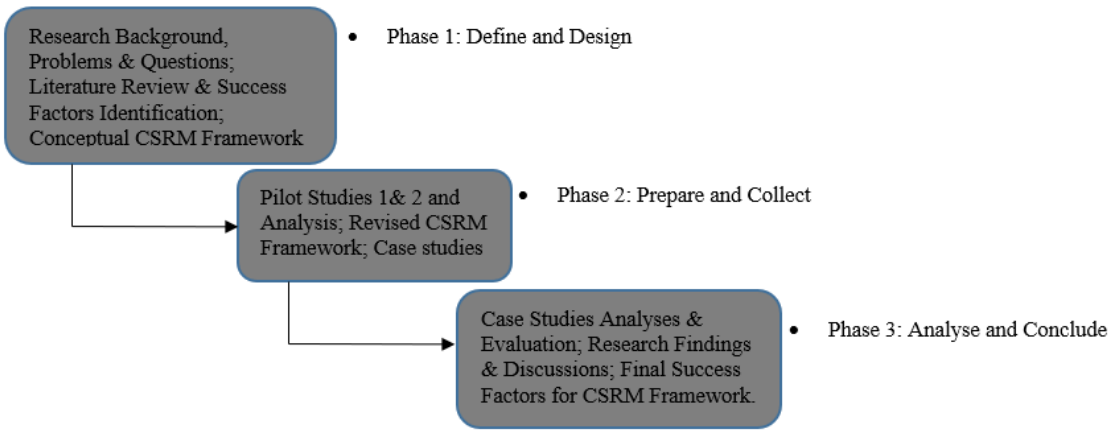

Figure 4.1: Research Development Phases

The design started with the initial collection of the background information on the topic and found the relevant literature with the extensive literature search process described in section 2.6. This step is accompanied by the critical examination of the current relevant literature on CSRM implementation success factors. Further, it results in the identification of the research problem. The research questions that would then direct and focus the study were created during the relevant literature review. This inspired the categorization, development, and proposal of an initial conceptual framework from high-impact themes related to factors generated from the literature review of related studies in information security/CSRM. The latter in chapter 3 discusses the proposed empirical research.

Phase 2 continues with two pilot studies from similar case organisations to the data collection, collation, and analyses to generate the ultimate refined framework. This study adopted multiple case studies. This approach is more robust than conducting a single case study despite multiple case studies being more energy and time-consuming than one case study. Multiple case studies are commonly thought more robust, with more convincing results (Yin 2003). However, the case study as a distinct method of social science inquiry is not without some concerns. Such include lack of rigour in sampling, data collection and analysis due to the unimaginable comfort level as a case study can take too long; generation of a large quantity of data and unreadable documents (Rogers 2000; Yin 2014).

Feagin, Orum and Sjoberg (1991) in Yin 2014 dispel these myths by pointing out that conducting a case study for a long time is a thing of the past, not the present or future. He posits that information from many studies for an extended period thus permits a holistic study of a complex web of social interactions-social action, social networks, and social meanings. The research design translated into an actionable plan in successive stages of the study to investigate the factors further beginning with the pilot interviews based on (1) transforming the task of data collection in a detailed and controlled manner; (2) ensuring the collection of appropriate data that relates to the events or explain features and abilities within a CSRM implementation success process; (3) ensuring a clear strategy for the achievement of the research objectives.

The collected data were analysed, and relevant success factors for CSRM implementation in practice and their interdependencies result in the comprehensive model of success factors for CSRM implementation in the final phase. The data collection process is discussed as follows.

4.5.2 Data Collection Process

The overall data collection followed two phases. Two pilot studies were conducted as part of the research process to refine and improve the mechanism for data collection in the first phase. The second phase was the implementation of the pilots for the actual case studies. The first semi-structured interview pilot study was conducted in the UK at two e-retail organisations in their locations and four colleagues within and outside the Coventry University campus within a month. The second pilot was done in Nigeria because the methodology study context changed from the UK to Nigeria after the first pilot (See section 5.2 for details).

The choice of case study is to have an in-depth understanding of the identified factors and how they enhance CSRM implementation success. Finally, it validates the framework. The aim and the interview outline were discussed with the participants. Also, it assures them of the confidentiality and privacy of data collected during the interview session. Data of CSRM implementation case studies' success factors were collected primarily using the individual semi-structured interview method because the interviewees could express their meanings and interpretations through their discussions (Ritchie et al. 2013).

The predetermined, semi-structured interview question is best suited for a qualitative study exploring success factors for CSRM implementation in Nigeria (Brinkmann and Kvale 2018). More follow-up questions were used for clarifications or detailed explanations of the responses given in the semi-structured interview. Other data sources, including documentation from E-retail staff and the regulatory Bank, and external sources provided more information on success factors for CSRM implementation. Therefore, this research adopted method triangulation for practical explanations to provide the empirical evidence supporting findings arguments (Flick 2018).

The interviews were conducted with relevant personnel of the organisations directly involved, with life experience in CSRM implementation strategy and related activities and operations, which primarily included IT, risk management, audit, and compliance (Kayworth and Whitten 2010). The identified gatekeeper was the principal contact in all the organisations that helped identify the right participants. The interviewees used snowballing technique to refer more participants. The gatekeeper varied among the four organisations ranging from the CISO to the Compliance manager.

The gatekeepers introduced the researcher to the participants in most cases. At the same time, people management skills paved the way for direct collaboration with the interviewees to schedule interview meetings at their convenience via Skype and telephone conversations. The data collection approach was not without challenges, such as several calls and reminders to participants to grant the interviews. Sometimes, the meetings were cancelled and rescheduled to late in the night with no choice but to adapt for more explanation at their convenience. These challenges were not surprising but prolonged the phase of the research. The staff, especially those in CS departments, have strong work ethics and enormous demands considering the escalated cybercrime cases in Nigeria.

The participants received emailed letter of introduction (See Appendix A) containing the research background and objectives before the interviews. No interview was conducted without the interviewee's consent, and most of the interviewees preferred taking notes to be recorded. This approach made the process very challenging, relying on the notes taken. Based on the prior experiences from the pilot interviews, excellent listening skills to interviewees have been developed. This helped comprehend their responses, distil the meaning from answers and link different answers. Restating or paraphrasing responses and seeking confirmation was employed as part of reflective listening.

The research topic and interview background questions were introduced during the interviews. Discussions progressed with the interview questions that served as the topic guide related to success factors for CSRM implementation. The guide led to live interviews, phrase questions and engage the interviewees based on interview circumstances. It facilitated the systematic exploration of the key topics of success factors of CSRM implementation and allowed flexible investigation of the case studies. It also prevents bias and ensures consistency in the participants' responses to the questions. Relevant and valuable data can only be obtained without prejudice when interviewees give personal views in response to similar questions asked each participant.

Overall, the participants responded in a friendly atmosphere, and the interviews went on smoothly. However, there was no apparent need to ask all people general questions such as the overview questions. Since many topics were covered, it was unusual for an interviewee to have complete information about the CSRM implementation in all sections. Hence, this study focused more on the areas relevant to the participant's different roles to describe their experiences differently and in detail. This allowed the opportunity to use in-depth interviews to provide

flexible, interactive data collection to generate and capture the depth and rich data in its natural form.

The minimum time for the interview was 35 minutes, while the maximum was about one and a half-hour. Necessary documents referred to during the interview discussions were emailed to the interviewer. Generally, the data collection's depth was encouraging, made the interviewer very happy and thanked all the organisations that participated for their cooperation.

4.5.2.1 Interviews

Denzin and Lincoln (2012) regard interviews as the primary qualitative research tool for data collection. Yin (1994) regards interviews as one of the essential sources of case study-based research information. Since this research chose the interpretive stance, it considered interviews the primary and appropriate data collection source. Literature indicates that interviews allow the best access to the: (a) interpretations that the participants have regarding the actions and events which have or are taking place and (b) the views and aspirations of themselves and other participants (Walsham 1995b).

There exist different forms of interviews. There are three main types of interviews, according to Denzin and Lincoln (2012), namely: (a) unstructured, (b) semi-structured and (c) structured. Interviews take several forms like face-to-face group interviewing, personal interviews, telephone surveys, and more. The semi-structured interview was based on the interview agenda (Appendix B) to meet the research objectives. The semi-structured interviews presented flexibility in the research process, where the interviewer and the interviewees well understood the questions. The respondents answered specific questions on success factors for CSRM implementation.

All the interviews took place at the agreed time at the convenience of the interviewees. Case studies (A, B, C and D) influenced the research objectives' ability. Hence, the four selected case studies' characteristics typified the topic under study, whereas they control diversity to explore the influence and interdependency of various aspects of CSRM implementation success. The purposive sampling of case studies and participants was based on specific criteria for extensive data collection, providing an in-depth understanding of various organisations, and enabling comparison.

Validating success factors for CSRM implementation through the semi-structured interview protocol was designed to gain insights into participants who have hands-on experience and are actively involved in CSRM in the four case organisations (Elo et al. 2014; Reybold, Lammert and Stribling 2013). Also, to provide further context on perceived success factors and measures undertaken for CSRM (Magnusson and Marecek 2015). The most suitable participants in each participating organisation were on the criteria that the interviewees could answer the research questions through their personal work experience and views based on the study area.

Qualitative research is better focused on in-depth data collection coverage instead of breadth of sample size (Ritchie et al. 2013). This study concentrated more on the comprehensive data collection than the extensive range of the participants. The staff interviewed were comprised of lower-level staff and management staff to obtain both levels' perceptions. The interview agenda (Appendix B) focused on collecting data as follows:

Part A – General Background: This section seeks to obtain background knowledge about the participants' job function and years of experience and the overall view of the case organisations' CSRM implementation.

Part B – **E**: **Discussions on CSRM Implementation Success Factors:** The data collected addresses objective two and the research questions with the major factors discussed in sections 3.5 and new factors identified during the discussions.

Part F: Aims at reviewing the framework created in section 3.3 and the new factors to develop and propose a model for success factors for CSRM implementation in large organisations – Objectives 3 and 4.

The agenda covered all the important research problems described in chapters1-3. They dealt with identifying, evaluating the factors, and developing the model of success factors influencing CSRM implementation in large organisations. The participants' careful selection criterion was the achievement of a breadth coverage of the key participants correlated to CSRM implementation in those companies.

Thirty (30) participants of the case studies were carefully selected and interviewed and related aspects of the case study as applicable in Table 4.2:

Table 4.2: Participant's Profile

Years of Experience	Gender	Roles			Total
		Lower Management	Middle Management	Senior Management	
1-4	Male	7	0	0	7
	Female	1	0	0	1
5-12	Male	1	13	0	14
	Female	0	2	0	2
13-20	Male	0	0	6	6
	Female	0	0	0	0
Total		9	15	6	30

From Table 4.2 above, the carefully selected participants, three females and 27 males, were snowballing from the gatekeepers' recommendations and other participants as subject experts with relevant years of experience in the research area (Creswell 2017). They were chosen based on their relevance towards answering the interview questions (Bryman 2015) from the lower, middle, and senior management levels for balanced, unbiased, and rich information, which was an opportunity too good to miss (Bryman 2015). The participants included the chief security officers, lead implementers, security risk managers, data security analysts, human resources employee, security control, compliance and legal managers, user support officers, and regulatory authorities, network engineers, and business continuity employees were the first subject matter expert in at least one of the organisation's socio, technical and process disciplines identified in the initial framework from the literature synthesis. At 23, there was data saturation based on the responses from the three case studies. Advancing to 30 was to incorporate the broad overview of the regulatory organisation's experience, including the operative banking arm. Thereby performing a dual role in corroborating/disputing others' experiences based on their oversight functions and adding value to the study. It created diverse participants across case studies with possible cross-validated substantial results with empirical data's theoretical saturation.

The following subsections describe the current research context and the selected four case studies.

4.5.3 Choice of Case Organisations

In case studies and qualitative research, selecting the research participants constitutes a part of the research design. Samples could be probability or non-probability (purposeful). Many factors such as research aim, existing knowledge, theories in the field of study, contributions to knowledge or propositions to explore in the research (Ritchie et al. 2013) informed the decision to choose purposive sampling. The purposive sample of four organisations was based on the

objectives to gain different perspectives on the process (Creswell 2018) and the concept of information power (Malterud, Siersma and Guassora 2016). The study used a case studies strategy to gather retrospective accounts of successful CSRM implementations that would unpack meanings, aid understanding and generate themes and theories.

This research chose a qualitative approach based on two-stage criteria comprising organisational and individual stages since the study shares organisational research characteristics. The organisational phase focused on identifying the characteristics of four large organisations with headquarters or branches in Nigeria. The choice to obtain data from four case studies for comparative study rightly aligns with the methodological literature on qualitative case studies research to sufficiently achieve the research objective of evaluating success factors for CSRM implementation in large organisations in Nigeria.

Apart from the highlighted points above, large organisations are the prime target of unscrupulous fellows for monetary gain (section 1.4). Consistent with previous studies in the security field, the organisations deemed 'large' believed that such organisations would have relatively matured CS functional structures and groups and structured CSRM implementation processes (Colicchia, Creazza and Menachof 2019; Kayworth and Whitten 2010). Large firms usually have intense activities in the CSRM, more mature CSRM processes and technology in place (Yaraghi 2011). They have many assets, manage extensive information and data and the Triad (CIA) vulnerability that could be exploited, used or sold, cyber security programmes; these organisations are prime targets of threat actors (Aladenusi 2021).

Many authors believe that certain factors, including the high cost of risk management, impede the successful implementation of CSRM practices in organisations (Fraser 2016; Zhao, Xue and Whinston 2013). Hudin and Hamid (2014) believe that large organisations with high net profit adopt and implement state-of-art risk management practices. These organisations were also identified through a third-party consultant and web reviews' objective ratings to ensure they were effective in their CS approach (Kayworth and Whitten 2010). The ratings and reviews show how each company's CS program was judged to be comprehensive in terms of having an overall security strategy, low level of reported cases of fraud and breaches and over 1,000 employees. Therefore, large organisations satisfy an adequate territory of exploration for this study.

E-retail organisation and Banks were specially selected to make a diverse but complementary universe for case studies of a focused matter of similar outcome. The banking sector is the

Nigerian economy's central nervous system and has remained ever so pervasive in CS challenges of technology disease of internet fraud and cybercrime (Goni 2019). Furthermore, comparing similar cases and improving results' generalisability motivated the choices (Walsham 2006; Yin 2018. These selected companies operate in businesses with a similar degree of dynamicity and sufficient complexity of the organisation's competitive environment. They present homogeneity of CS risks, threats and CSRM management approaches regarding IT resources and roles. The possibility of accessibility and collection of information through direct interviews or indirect sources of information that could lead to richness of data were considered to perfect the selection.

Subsequently, some qualifying organisations that satisfied the above criteria were approached through professional colleagues and heads of cyber/information security through the LinkedIn social network. The gatekeepers assisted in presenting the permission request letter of the Coventry University to the organisations. These four case studies that obliged to participate in the research were denoted as Case Study A, B, C and D and described in section 5.3. To the best knowledge of this study, no previous case study researched success factors for CSRM's successful implementation in Nigeria.

4.5.4 Data Analysis

The immersive information from the empirical study of success factors for CSRM implementation success in Nigeria and data collected were analysed using thematic analysis to appreciate its richness (Boyatzis 1998; Magnusson and Marecek 2015). Thematic analysis was considered helpful in meeting the research needs due to prior knowledge of the qualitative research methods discussed in Section 4.3 and the insight gained from discussions in section 3.4 about the CSRM framework.

As a qualitative research technique, thematic analysis helps understand, interpret, and analyse the transcribed data from interviews from the case studies organisations (Vaismoradi et al. 2016). Key elements of the data during Qualitative data analysis resulted in identifying the themes, i.e., people, technology, process and organisational factors and derived concepts from socio-technical theory and conceptualisations of cyber security risk management, which helps for broader analysis (Bazeley 2013; Jackson and Bazeley 2019; Lewis 2015). NVivo software as a qualitative data analysis tool was preferred because it does not automatically code data into themes but permits visualising the data and deciding common themes (Edwards-Jones 2014).

This approach appeared suitable for framework evaluation and defending the research result. The cross-case synthesis validates each case study's outcome since multiple case studies are involved, and more success factors have been identified in the interview data (Yin 2018). The systematic case study protocols, rules of evidence, organisation documents for consistent data collection and cross-case synthesis address the study's validity and reliability threats (Yin 2013).

Hence, this research makes use of NVivo 12 software for thematic analysis as an analysis tool to break down the narrative aspects of success factors for CSRM implementation case studies through identifying themes and constructing concepts to meet the research objectives and provide answers to the research questions (Boyatzis 1998; Vaismoradi et al. 2016). The software facilitates qualitative thematic analysis, simplifies the coding, analysis, and view of data. Therefore, it grounds the analysis of the interviewees' explanations as it endeavours to link the interpretation with data. It is valuable in working with large volumes of data, promoting research reliability and validity.

Figure 4.2 depicts the thematic process containing eight stages from extant literature with several activities. Qualitative findings of success factors for CSRM implementation in Nigeria result from raw interview data.

This item has been removed due to 3rd Party Copyright. The unabridged version of the thesis can be found in the Lanchester Library, Coventry University.

Figure 4.2: Qualitative Thematic Analysis Process (Source: Adu 2019)

These stages are:

- Data cleaning: This stage's significance in understanding the collected data and creating ideas contributed to coding. This involves familiarisation with the interview transcripts in the form of a word document developed from the field notes and the memos (the documented personal observations, reflections, and impressions) by reading the interview

transcripts to gain an overview of the data and immerse in the entire responses from the raw interview data. The transcripts were stored in the computer as computer files. Also, the identified emerging inductive themes were used in later stages to label, sort and synthesise data.

- Upload of data into NVivo 12 software: The data (word document) was uploaded into NVivo 12 for thematic coding of relevant information for Case Studies A to D. Success factors for CSRM implementation was developed as the anchor code to help organise the coding system and identify the interview questions that directly addressed the research question.
- Reorganise the data into nodes: success factors for CSRM implementation form the primary node upon which other nodes developed. Numerous codes in the form of word text and phrases were identified from the collected data, such as business alignment, top management support, corporate governance, and many more. These codes were examined for any related concepts and relationships with each other. This was necessary to develop defined categories and themes based on similarities.

  The codes were created from the literature's themes and assigning relevant concepts confirming or disapproving them from the empirical data set. Also, generated emergent themes through inductive coding of the interview data from each case study. The data were grouped into existing factors or new factors. The themes created were reviewed to determine whether the developed themes have appropriate data. Bazeley (2019) and Gibbs (2002) expect in-depth and robust thematic analysis findings to support explicit arguments. This method improves the research quality, contributes to data validity, and enhances its credibility as it permits tracing the research conclusion (Hair 2015; Siccama and Penna 2008).

  The main categories - People, Organisation, Process and Technology were developed as parent nodes (main themes), while business alignment, corporate governance, management support, and many more form the child node (sub-themes).
- Explore imported data: explore possible themes related to the previously coded data from the earlier stage using ‘query’ commands such as training and policies. These themes often combine to create stronger links such as increased CS capability, effective leadership, and communication.
- Coding: The coding of the themes allowed the discovery of similar experiences of each interviewee (Leedy and Ormrod 2019). The themes generated were reread and reviewed to determine whether the developed themes and sub-themes have relevant data by

categorizing insights and experiences in synthesised data — for example, the people category is the main theme and awareness as sub-theme. This is a crucial stage in which relevant information in the data is coded after the data have been grouped into appropriate themes to address the success factors for CSRM implementation.

- Visualising: visually defines, refines, and conceptualize the content of imported data, generated codes, and themes through the confirmation of each theme to address the research question. For example, visualised each success factor for each case study using the project map and synthesised each participant's responses.
- Exporting: NVivo outputs from the project map are exported directly into the data analysis and findings discussions.
- Communicating: The thematic analysis findings are presented and discussed in Chapters 5 and 6. The data analysis results, findings and conclusions of success factors for CSRM implementation are communicated with clear arguments and address the research question. The thematic analysis approach helped this study have a broad framework to start the data analysis. This study can also link the study results and findings to the body of knowledge in the extant literature review of chapter 2 (Saunders 2016).

4.6 Data Triangulation

Triangulation is a process of taking different perspectives as corroborating evidence in answering the research objectives in qualitative research (Flick 2018). This research adopted methodology triangulation to produce new knowledge at various management levels, descriptions using several methods of data collection (interviews and documents), and themes in qualitative research to endorse the quality of this research (Creswell 2013; Flick 2018). Four quality measures considered for evaluation are credibility, transferability, dependability and confirmability (Lincoln and Guba 1986).

The study's credibility is assured by triangulation to ensure that the study measures what is intended. Triangulation was achieved by cross-checking data (collecting data from different sources) or interviewees with contrasting perspectives to verify and compare the different viewpoints and yield better knowledge. Also, comparing the pieces of evidence from multiple sources achieved literature triangulation (Yin 2013). Thus, comparing participants' responses and results from the four case studies (as reliable sources) and corroborating the findings of prior related studies on CSRM implementation experiences in several other large organisations.

Also, the credibility of frequent member checks and debriefing sessions with stakeholders and supervisors to review the research processes ground the findings to the collected data by describing the analysis process and building trust with the interviewees. The interpretations were presented to some respondents to obtain feedback on the findings to enrich the understanding. The review and validation of these success factors by first-hand experienced industry professionals in CSRM provided credibility to the results. Moreover, thematic analysis, a well-established research method, ensured the research process's high credibility and qualitative studies analysis (Vaismoradi et al. 2016).

The second criteria, transferability, i.e. the extent or degree of fit of the applicability of all or part of the findings elsewhere, was achieved by providing detailed background and demographic information of the different case organisations and interviews (Lincoln and Guba 1986). The third criterion, dependability, use techniques to record the research process for consistent results if repeated in the same context using the same research methods by an external auditor (Lincoln and Guba 1985). Table 5.1 shows the research context and participants' profiles to ensure transferability. This chapter presents a detailed description of the research process and design by explaining how the data collection and analysis were performed to establish its high quality consistently.

Finally, the confirmability criterion judges the research flow from data collection to articulating the research findings (Lincoln and Guba 1986). Impact and importance constitute essential factors in maintaining the interest and attention of the readers in the research. Triangulation as a piece of confirmatory evidence reduces study bias (Creswell 2018). A clear and extensive discussion of the thematic analysis methods allows grounding the analysis in the participants' accounts from four case studies (Yin 2013) and audit of research conclusions. The commitment to consistency between the chosen research paradigm in subsection 4.2.2 and the research data collection and analysis described in subsections 4.5.2 and 4.5.4, respectively, implied the adoption of trustworthy criteria and high research quality.

4.7 Research Products and Presentation

The research outcomes are Research Products. Research outcomes contribute to knowledge, including theoretical and practical implications in the last chapter (conclusions chapter). Also, products include the thesis addressing the research question. Research presentation is how the research is explained and disseminated to readers (Oates 2005). The current thesis structure is

typical of a thesis made appropriate by collecting relevant evidence, justifying research methods selection, reflecting the research process, supporting evidence, creating new knowledge, and using the Coventry reference convention.

The findings, quotations from the data and data interpretation are combined to present the qualitative analysis findings by following the suggestion for writing and evaluating qualitative interpretive case study findings (Myers 2019). The comparative cluster analysis frequencies report improves data reliability and validity. It is not unusual to expect the unexpected in qualitative case study research and justify the exigencies and rigour in writing. Therefore, the writing style comprises two components: plausibility of the story and overall argument. Data extracts (evidence supporting argument) and verbatim quotes bring the case to life and discursive commentary (discuss how data extracts support the argument) in an engaging manner with sufficient evidence. The careful interpretation of the data with successive member checking derives the study's conclusion. The thesis was carried out professionally and written to present the current study as the hallmark of quality qualitative case study research.

4.8 Ethical and Privacy Issues

Research ethics forms part of research design (Oates 2005). According to the university research procedure, a formal ethics approval request from the University ethics department before starting any data collection. Permission to commence the research was granted from the Coventry University ethics committee to interview participants of success factors for CSRM implementation case studies. The ethical approval was presented to the gatekeepers. It prevented any ethical dilemmas about the research's sensitivity, especially the participant's identity, that may restrict access to quality information.

Participants received a letter of invitation and an informed consent form with full explanation and information about the interview objective, the usage of collected data, the expected duration of the interview and the participant rights to address any ethical and privacy concerns at the commencement of the interviews. The majority of the participants readily accepted the invitation letter and helped reduce the participants' risk of no cooperation. Also, despite the risk of insufficient data collection that is time-bound, the detailed invitation letter helped gain the participants' confidence and assurance of anonymity and confidentiality to discuss freely with the interviewer.

The study was committed to the participants' consent and assured anonymity of interviewees' data (Oates 2005). Since the research method focused on interacting with human life experiences and organisations, only collected the essential demographic-related data to avoid compromising participants' anonymity. Transcripts and data analyses were managed in a way that did not compromise any participant's anonymity. The four organisations investigated in this study were coded as Case Study A, Case Study B, Case Study C and Case Study D. The interview notes were transcribed quickly into electronic formats to avoid the risk of any confidential information exposure. The interviews are kept secure and safe in a locked cabinet, and computer files are password but accessible only for research purposes.

4.9 Chapter Summary

This chapter aims to propose a justification for using an appropriate research methodology for this thesis. The chapter presented the research methodology, discussed, and justified its epistemological view and suitability (the interpretivism stance) for this thesis. This decision is because of the aim and objectives of this research, as described in Section 1.5. Then, discuss the quantitative and qualitative research approaches. This study chooses a qualitative approach within this study's context to be appropriate for the reasons explained in Section 4.3. Section 4.3.1 highlights such reasons.

Section 4.4 outlines the available research strategies and justifies the case study strategy's choice to be appropriate for this research in Section 4.4.1. Moreover, this research uses multiple case studies to explore and understand the success factors for CSRM implementation in Nigeria. Also, it outlines and discusses the research methods and provides arguments for the suitability of the methods. Thus, various data collection methods used include, among others: (a) interviews, (b) documentation, (c) internet sources. Then, Sections 4.5, 4.5.1, 4.5.2 reported the empirical research methodology followed in this research, the research design and the data collection process incorporating the case study protocol. This protocol is a valuable tool that acts as an operationalised action plan for empirical enquiry. This study used case study perspectives to allow others to relate their experience to this research outcome based on this protocol. Section 4.6 presents data triangulation. After that, Section 4.7 presents the thesis's outcome to provide a broader understanding of the success factors for CSRM implementation in Nigeria.

The chapter presents the methodology for the study and the sequence of activities. Previous studies and existing literature on research methods helped select the best methods for evaluating

success factors for CSRM implementation in Nigeria. The method was essential to answering the research questions, allowing the extension of the socio-technical theory concept applied to CSRM implementation success in Nigeria.

The rationale for choosing the research method, interpretive research philosophy and case study strategy was justified. The qualitative research process of data collection and analysis answers the research questions. The successive chapters of the thesis highlight the findings from the case studies. These success factors were subsequently investigated in different phases of the research, beginning with two pilot studies, first, at the end of Phase 1 and the second at phase 2 detailed below in subsection 5.2.2 and 5.2.5, respectively. It is necessary to state that these two stages were not linear.

Conducting an initial pilot study in this stage provided feedback to the first stage that enhanced the slight change in topic from the Evaluation of Cyber Crime Risk Management (CCRM) approaches in E-retail organisations in the UK to evaluate success factors for CSRM in large organisations in Nigeria. The change led to pilot study 2, the selection criteria and data collection protocols for the case studies in phase 2. Then, case studies were selected as described in Section 4.4.1.
Participants and designed data collection instrument described later in Subsection 4.5.2, titled Data Collection Process—conducting initial fieldwork provided feedback to the first stage that enhanced the selection criteria and data collection protocols in phase 2.

In the multiple case studies phases 2, namely, prepare and collect stage, this study presents and analyses the empirical data collected from four case studies in Nigeria. The below subsections 5.3.2, 5.3.3, 5.3.4 and 5.3.5 portray these case studies that provided enough beneficial information that helped justify the research presented in this thesis. It is essential to state that both stages were circular research processes. The objective was to present the preliminary research findings obtained while engaging with the staff in real-life organisational settings.

The data collected validate: (a) the proposed CSRM implementation success factors (Figure 3.1), (b) the socio-technical factors for CSRM implementation success. Nevertheless, the analysis of the empirical data does not assume the comparison of cases. Conversely, this chapter covers the empirical analysis of four case studies viewpoints that explain people, processes, technological and organisational factors that influence CSRM implementation success.

Consequently, rather than generalising the results of these cases, this study examines each case study by analysing the findings and comparing the findings from each case study, in doing so, allowing others to draw parallels in the outcome. This chapter commences by discussing the two pilot studies, subsequently providing the background to selecting the four case studies in large organisations in Nigeria. The chapter then moves to a detailed presentation of the four case organisations. The empirical results derived from the case organisations have confirmed the conceptual model's validity in chapter 3 with interpretations and explanation images.

Finally, in the third stage (analyse and conclude), the four case studies were analysed in Chapters 5-6. Chapter 7 provides the findings of the analysis.

Chapter 5: Case Studies Findings and Analysis

5.1 Introduction

The chapter elaborates the success factors for CSRM implementation in four purposely selected case studies in Nigeria by applying the chosen research methods consistent with the proposed theoretical and conceptual frameworks (Figure 3.1). The empirical data collection was from the primary (verbal) and secondary (shared documents) from one e-retail organisation, two financial institutions offering related services and a supervisory and regulatory institution.

The chapter advances further insights on the success factors previously identified in chapter two to achieve the research aim to explore the factors that facilitate CSRM implementations success through several practices. Also, the chapter describes, discusses, and evaluates each case study. The case studies endeavour to understand the success factors influencing CSRM implementation from 30 participants, including each factor's primary activities. The discussion adopts three elements: data, broad explanations, and arguments. The comprehensive explanations discuss data (presented in italics) in the argument context, while the arguments and explanations are presented in standard text. Each argument signifies the data analysis findings, supported by a quotation of the data to illustrate how the arguments ground data.

Questions about the participants' views to confirm CSRM implementation success in the organisation and measures to ascertain success set the pace for the interview process at introduction. Although evaluating whether the organisations are successful is not the aim of this study. These two form the central theme of the first part of the semi-structured interview section. The thematic analysis in this chapter presents the emerged themes from the framework analysis of the case studies.

5.2 Phase 1-Pilot Studies

The pilot study tests whether the data collection instrument design is appropriate for answering the research questions and objectives (Doody and Doody 2015). Also, it verifies the appropriateness of the interview protocol, the data collection and reporting systems (Yin 2009). Hence, the data were not included in the empirical data for the actual four-case studies analysis.

Table 5.1 shows the second pilot study report conducted with three participants from Nigeria within a week.

Table 5.1: Pilot 2 Participant's Profiles

Organisation	Professional Role	Mode of Interview
E-retail	Head Enterprise Security	Skype
Bank	Head Cyber Security Audit	Skype
Information Technology and Services	Cyber Security Manager	Skype

The participants' feedback on the interview process assesses how easy it is to understand the questions at the end of each interview to establish credibility (Wilson, Roe and Wright 1998). The researcher carefully transcribed the participants' responses.

Problems and lessons learned from the pilot study are:

- Barriers to getting interview participants**:** The pilot study highlights the need to devise a new strategy for getting participants.
- From an investigative and interpretive researcher perspective, self-engagement in an appropriate corporate, social, and cultural way: Upon reflection, the interviewer became confident with excellent interview skills as the interview progressed after the first interview.
- Modifying interview questions: The need to modify the questions to make them easy to understand. However, the practitioners will be better suited to answer the questions.
- Removed repeated questions: The pilot study's understandings helped modify the study's main interview questions for participants to express their views and describe their experiences effortlessly. Asking intelligent questions about CSRM implementation is critical to the study (Power 2011).

5.2.1 Population Sampling and Data Collection Phase 1

In qualitative research, sampling starts with defining the selected portion of the population (sample) for an investigative purpose (Bryman and Bell 2015; Hair 2015; Sekaran and Bougie 2016). After careful consideration of the rationale and criteria for sample selection, purposive (non-probability) sampling was employed, common in qualitative research (Malterud, Siersma and Guassora 2016). The interviewees must possess the research topic's personal experience, willing to discuss and share in-depth information-rich views.

Before the commencement of the case study, efforts were made to align the research purpose by contacting participants who had adequately addressed the business problem (Elo et al. 2014;

Reybold, Lammert and Stribling 2013). A senior manager of British Retail Consortium, Internet Retailing organisation and staff in the financial industry were sources of introduction and possible snowballing to e-retail organisations. The target sample (decision-makers, junior teams, and implementers of CSRM approaches) have already responded positively to their cooperation, having listened to them discuss CSRM related issues in a webinar in 2018.

Thirty interviewees directly involved in the operations, technical and risk management aspects of three case organisations (10 each) expected proved challenging to achieve. Stuart et al. (2002) and Yin (2014) suggested one-three case studies, while others suggest four to ten (Eisenhardt 1989). Typical of the difficulty of obtaining data in other information security and CS fields, information may not be freely shared due to this topic's sensitivity (Alawonde 2020; Baskerville et al. 2018). Snowballing enhanced data gathering. Purposive sampling facilitates identifying patterns across organisations, thereby strengthening the findings' reliability and validity.

5.2.2 Pilot Study 1 and 2 Challenges

The researcher collected data from three individuals from different companies within four months of continuous visits, several telephone calls and e-mail reminders due to this topic's sensitivity in freely sharing information. Despite the small sample size selected for the UK E-retailing organisations' interviews, accessing the organisations was difficult. Efforts were made to change the data collection method from interviews to surveys. Still, the researcher was depressed with the risk of not getting more significant responses (250-300 average) required for quantitative research.

Furthermore, conducting an open-ended questionnaire during pilot 2 yielded an inadequate response from participants due to the lack of time in typing responses and the ease of finishing quickly. In-explicit answers were challenging to identify the success factors, requiring more un-intended clarification to understand and interpret the study's subjective details. Hence, the Director of Studies approved modifying the topic and the context to Nigeria, knowing that cybersecurity has no geographic boundary. The research design is meant to achieve the intended purpose. The researcher had successfully obtained the consent of two case organisations for their cooperation. The research question, literature review and conceptual framework were subsequently modified as explained in chapters 1, 2 and 3.

5.2.3 Pilot Study 1 Analysis

The following themes, not pronounced before the interview, emerged during the manual analysis and discussions of the pilot interview.

- Trust: Customers trust or rely more on anti-virus installed on their computers as complete protection against cybercrime risks. These attitudes or beliefs corroborate that humans constitute a challenge to CCRM implementation.
- Time: E-retailers do not usually devote time to training staff at the branch level about CCRM but concentrate more on health, safety, and store management.
- Organisations do not speak the same language across the branches. Staffs at branches are naïve about CCRM. They believe that technical skills and expertise are needed most at head offices — simple process such as logging off profiles after work is still a challenge in some branches.
  The E-retail branch manager commented:

  You cannot own what you do not know.

- Old technology and practices at the branch level; customer data is highly vulnerable to attack. Since there is no attack yet on an organisation, there is complacency that it is doing well, and subsequent investment in system upgrades is minimal.
- There are disconnections between what management thinks about CCRM implementation and employees' perceptions of those implementations.

5.2.4 Research Question Formulation and Interview Questions

The main research question focuses on the study: What success factors influence CSRM implementation? The case study addressed the relevant research question in Table 5.2
below.

Table 5.2: Interview Question

Research Question	Case Study Objective
Question 1: What are the factors that influence the successful CSRM implementation in your organisation?	The literature review phase identified some factors, which required validation during the case studies. These questions divided into six parts, A and F. Part A covers the CSRM implementation in participants' organisations and the participants' experience in implementing CSRM. While the questions in part B-F centre around eleven CSRM success factors.

Chapter one outlines the research objectives used to construct the interview questions for the case studies. The questions were adopted and adapted from similar studies to suit this study. Table B1 (see Appendix B) shows the summary and description of the eleven factors that made up the interview questions. Appendix B summarises the participants' interview questions based on the description of success factors in table B1. The pilot study's detailed data analysis helped ensure that the researcher became familiar with using NVivo 12 software for thematic analysis. The intention is to hasten the completion of the central case studies, findings and results analyses.

5.2.5 Pilot Interview 2 Findings

The interview recordings were carefully transcribed verbatim and later uploaded with the field notes as computer files into NVivo 12 software for thematic analysis. The pilot interview results showed that all the participants largely attest to clear wording and the appropriate groupings of success factors. For instance, participants A, B and C responded that*:*

> *Interview questions and the grouping were good, but the adoption of international standards and best practices like PCI-DSS, NIST, ISO 27001 are significant elements of CSRM (Participant A).*

> *Nothing much needs added, but Audit is a critical factor that helps us know how compliant we are to the process* (*Participant B*).

> *The interview questions pretty touch much on the critical factors. They are a giant umbrella for others* (*Participant C).*

The analysis of the participants' profiles (Figure 5.1) with the quality of information and responses provided showed their knowledge and experience within the study context, examining the success

factors influencing CSRM implementation in large Nigerian organisations. For example, when asked how their organisation measures their CSRM implementation's success. They were confident in discussing their experiences and views of their CSRM implementation success.

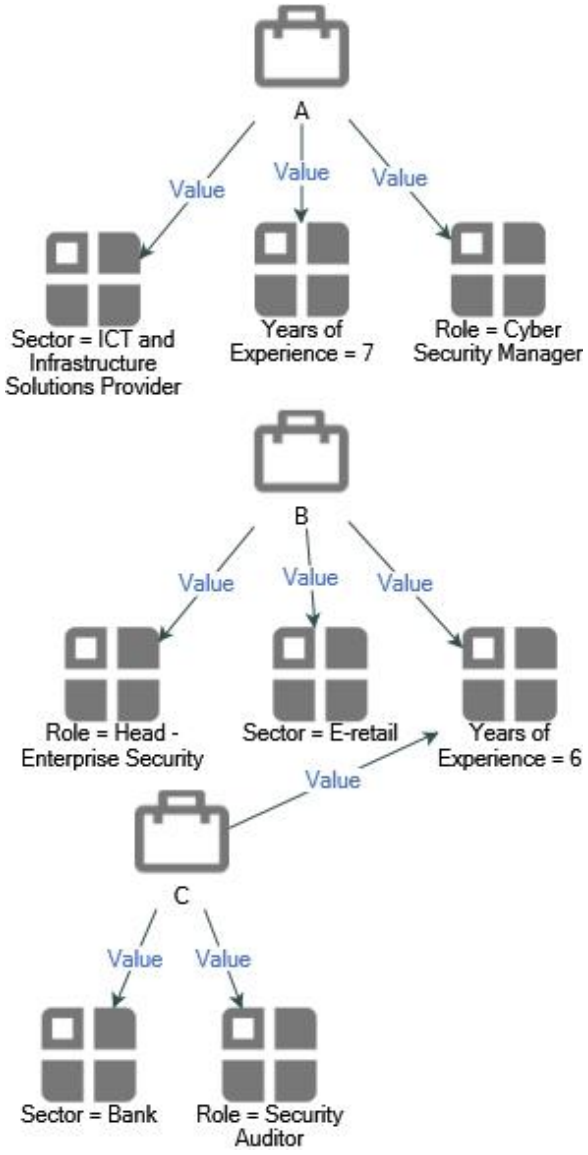

Figure 5.1: Participants Profiles

Figure 5.1 confirmed the possible suitability of the success factors in the CSRM framework due to the number of years of direct relevant experiences in CSRM. However, there were suggestions for improvements despite the positive feedback. Table C1 (see Appendix C) highlights the feedback review and the actions taken to improve the identified areas.

Based on these understandings from the pilot study, revised the main study interview questions to accommodate all suggestions (Table C2) in Appendix C.

5.2.6 Summary of the Pilot Studies

The pilot studies helped make amendments where necessary to avoid misunderstandings (Yin 2018). Reflections on the pilot studies allowed the first version of the conceptual framework for success factors influencing CSRM implementation in Chapter 3 to be revised. Thematic analysis of the interview responses supported the existing factors and enabled the re-grouping of the similar interrelated factors for CSRM implementation success. Also, some measurement constructs aligned with the success factors themes were discussed and identified as sub-themes that could be regarded as sub-factors. However, these factors were verified via semi-structured interviews involving 30 participants from four large organisations during phase 2-central case studies.

5.3 Phase 11-Main Case Studies

5.3.1 Background to the Case Studies in Large Organisations in Nigeria

The background information about a study context is necessary for any research writing (White, Woodfield and Ritchie 2003). This subsection presents the justification for the location, Nigeria. Also, it described the possible controls, including language, economic environment, culture, and legal system through the geographic area. More importantly, factors, such as legislation, regulations, and stakeholder pressures, vary among countries, leading to deviations in the analysis and results (Mena, Humphries and Choi 2013).

The exploration of success factors that influence CSRM implementation was conducted at four large organisations in Nigeria. Several reasons for this choice include; first, Nigeria is a developing country with many businesses embracing the gains of internet transformations due to their enormous benefits. Also, other scrupulous individuals compete to take their share, making Nigeria's cybersecurity situation vast and complicated for large organisations (Achumba, Ighomereho and Akpor-Robaro 2013; Goni 2019).

The alarming outburst of cyber-crime in Nigeria is disturbing, and CS in Nigeria is a perfect storm with global concern (section 1.4). Additionally, because of the significant investments

synonymous with IT and security and the country's economic situation, investments in CSRM are gradually increasing. Because of such tendencies, few organisations implement CSRM appropriately (section 1.3). Second, as explained in subsection 2.7, the literature reveals that previous researchers investigated success factors in related studies in other countries (Al-Awadi and Renaud 2007; Dzazali and Zolait 2012).

This research of success factors influencing CSRM implementations in Nigeria is unprecedented due to the lack of research in the subject area. Third, many economic and sustainable researchers call for a global perspective on security challenges in Nigeria for sustainable development (Aminu 2013; Achumba, Ighomereho and Akpor-Robaro 2013). This current study supports this trend by studying CSRM implementation success factors and cross analysing its findings with the related literature of CSRM research in other countries. Fourth, CSRM is a global issue with no geographic boundary, so the study context is valuable to promote cyber peace in Nigeria and worldwide (Avgerou and Walsham 2017).

The effective and appropriate implementation of CSRM is fundamental to all societies, with positive and negative features in all organisations. The goal of all should be mutual learning from each other, and the subject matter should be a topic of continuous vigorous research (Avgerou and Walsham 2017). Fifth, the level of computer and internet literacy in SMEs are shallow with fraud and security concerns. Most SMEs do not have e-retailing business culture, and an infrastructural challenge is a significant problem. Sixth, the ease in locating and accessing keen case studies culminate large organisations' choice, as discussed in section 4.5.3.

It is worth noting that all research contexts have cultural impacts resulting from people’s shared values and norms, language and literature based on their ways of talking, thoughts, and acts in a specific context. Nigerian culture would impact this research by way of communication, decision making and management styles. First, it is common to make decisions slowly and quickly downturn decisions. This attitude would lead to reliable decisions on factors that will enhance CSRM implementation success. Second, managers usually make decisions, while sometimes staffs wait to be forced or told what to do. This suggests that, in ensuring CSRM implementation success, employees do not question the decisions often backed with sanctions. Although, a participant strongly attributes their CSRM success to staff commitment, not the penalties.

5.3.2 Introduction to Case Study A

Case Study A represents an extreme of a successful CSRM implementation in Nigeria that would reveal learning aspects based on its long experience with CSRM and size. It is one of the fastest-growing and most prominent E-retail organisations in Africa. To corroborate this, the CISO stated that:

> *We have had continuously attempted breaches – none successfully penetrated yet in the last five years.*

The organisation is a reputable E-retail service provider that has operated for over eight years from the commercial hub and most populous state, Lagos, Nigeria. It fulfils the characteristics of a large organisation as a leader in revolutionising the retail industry in West Africa with over $500M revenue. It offers a wide range of products and clothes, beauty products, home appliances and groceries with more than 4,000 workers with distinguished customer service and satisfaction at the hallmark of its success in Nigeria.

Case study A prides itself on adopting effective best standard practices for security across its departments with dedicated teams of experts for operations and processes. Table 5.6 shows the seven participants' profiles to obtain multiple perceptions about the success factors for CRSM implementation. Additionally, few participants shared documents such as risk assessment and treatments processes and a list of CSRM implementation policies as a second data source.

Table 5.3: Case Study A Participant's Profiles

Participants	Role	Years of experience
P1	Chief Information Security Officer (CISO)	20
P2	Head - Enterprise Security	6
P3	Dev Ops Engineer	2
P4	Information Security Specialist	2
P5	Risk Manager	6
P6	Data Security Analyst	1
P7	Data Security Officer	1

Table 5.3 shows the participants' relevance to the study concerning their ability to speak and share their experiences on the success factors for CSRM implementation in their organisation. Subsequent sections discuss the case study findings from the NVivo outputs.

5.3.2.1 Success Factors for CSRM Implementation in Case Study A

This section addresses and represents the participants' views and understanding regarding the success factors that influence CSRM implementation in the organisation. The main question:

> *What factors are associated with CSRM implementation success in large organisations in Nigeria?*

The semi-structured interviews investigated the central theme (the study's main research question). The question intends to identify if the organisation had implemented the CSRM considering socio-technical components: People, technology, process, and organisation as success factors. The coding of the interviewees' responses births the emerging sub-themes denoted as child nodes in NVivo, highlighted in Table 5.4.

Table 5.4: Success Factors for CSRM Themes and Sub-Themes

Themes (Parent Node)	Sub-Themes (Child Node)
People Factors	• Top management support • Awareness • Training
Technology Factors	• IT Competence • System Quality (Task-Technology fit)
Process Factors	• Risk Management • Enforce CSRM Policies • Security Audit
Organisational Factors	• Business alignment with CSRM goals • Corporate Governance • Adequate Budget Planning

Detailed discussion and analyses of the themes and sub-themes are as follows:

5.3.2.2 People Factors

The People factors theme aligns with the definition in section 2.7.2. The stakeholders include all employees such as top management staff, CSRM implementation team, IT team and all end users of IT systems. Any CSRM system will have input from or be implemented by people (individuals) whose attitudes to risk may have a meaningful impact on the system's successful implementation (Hadlington 2017).

The analysis of case study A revealed all participants' exceptional importance of people factors in CSRM implementation success. Comprehending an individual's behaviours and attitudes, the surrounding context, and decisions made are vital for an organisation's operations success (Kamal et al.2015). Figure 5.2 shows the NVivo representation of the identified theme and sub-themes (top management support, awareness, and staff training).

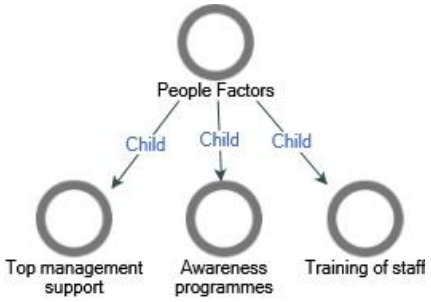

Figure 5.2: People Factors Sub-Theme for CSRM Implementation Success

The discussion of the sub-themes explains thus:

- **Top Management Support**

Top management support is pervasive in most security domain research in all organisations (Zammani and Razali 2016). The level of support and commitment from top management is dependent on their awareness, knowledge and understanding of CS and risk management concepts on CS. The resultant benefits will be successful CSRM implementation phases. Top management support is ranked as the most critical success factor for CSRM implementation success by all the participants because it cuts across all four significant themes.

The participants explained that Top management's involvement is critical in achieving the CSRM implementation program's intended outcomes. The thematic analysis shows that the top management has been able to demonstrate support in many ways compressed into eight sub-themes and discussed:

Leadership and direction: Top management leadership and direction plays a vital role in CSRM implementation success. Top management develops goals, strategic plans, company policies and makes decisions on the business's direction. P6 and P3 supported that:

Top management ***leads and directs*** *by* ***helping to drive the development and the implementation of policies and processes*** *by sending emails to all staff to comply, else apply restrictions (P6).*

Top management ***buy-in*** *and communicate active support by leading and joining weekly progress meetings to discuss issues and successes (P3)*

Formulates and decides objectives and strategies for CSRM and the business: Case study A being an e-retail organisation, the growing emphasis on CSRM is on a better strategy and methodology for securing information and information systems that are core organisational assets. Top management plays a key role in formulating comprehensive, clear strategic business goals, objectives and CSRM policies communicated to all employees and stakeholders to facilitate CSRM processes. The managers, IT, and support staff reiterate their CSRM implementation success to the top management staff's commitment and support. For example, P2 and P6 commented that:

Top management drives the CSRM implementation process and communicates its active support for CSRM by ***engaging CSRM managers*** *and* ***asking for a CS roadmap yearly (****P2****).***

Top management ***formulates and decides objectives and strategies for organisational risk management activities*** *to anticipate the probability of a negative impact. They engage* ***with the CS manager*** *to* ***help prioritise CS assets*** *and* ***make specific trade-offs between risk reduction and operational impact*** *(P6).*

Establishes the CSRM project management office: Implementing CSRM is synonymous with conducting a CSRM project. Organisational CSRM implementation success follows specific opportunities within the existing project management processes, such as information security management system implementation. CS risk management is a project involving a high amount of uncertainties of risk of failure; hence, diminished ROI or a loss of huge investment is one of the implementation challenges of CSRM.

Some researchers apply risk management tools and techniques to improve the information security management system implementation (Maarop et al. 2015), project risk management success (Raz, Shenhar and Dvir 2002; Zwikael and Ahn 2011) by establishing a project

management office to manage the implementation process. This comprises project management teams. However, risk management has always been a part of project work because of high uncertainty due to risks. The risk manager replied:

> *Top management support comprises various practices, including developing **strategic plans** such as the initiation stage, establishing a **project management office**, training programmes and much more.*

Budget approvals: Allocating a sufficient financial budget to get the tools and resources needed for CSRM implementation success is ubiquitous and ranked high in many security literatures. Effective and efficient resource management includes providing necessary human resources and skills and purchasing tools and techniques for CSRM implementation activities.

Budget approval by top management was rated critical by all participants by explaining the business opportunities CSRM implementation brings to the organisation. The evidence presented supports the idea that organisations today are only looking, confident to engage and partner with CSRM compliant companies as a prerequisite and requirement for business engagement. The best way to assure organisations and partners that the company can ensure shared Personal Identifiable Information (PII) data is secure is by providing an adequate budget, planned and approved for CSRM implementation.
The CISO with 20-year experience commented that:

> *Risk management requires acknowledging that risk is a reality. The commitment to identify and manage risk can only be successful when the top management is involved and an **adequate budget** is **approved.** He exclaimed that it is hard to **quantify the effect or impact of investments** in CSRM and the value an organisation derives! How can someone rate reputational damage?*

Effective communication*:* effective and timely communication with stakeholders is vital at different CSRM implementation stages. The root causes of most failures and uncertainties in CSRM implementation projects are traceable to ineffective communication among stakeholders. The organisation's CSRM implementation stakeholders are often from various departments, backgrounds, and languages. The responsibility is on top management to transcend the differences. Top management provides different robust and efficient channels (verbal, visual and written communications) to stakeholders to discuss the CSRM implementation process

requirements, issues, and progress reporting.
The data security analyst (P7) articulated that:

> *The top management support through the provision of the communications channel, effective governance, granular progress reporting on specific milestones in the CS programme helps push changes in frontline employees' user behaviours in understanding why they need to protect critical security/information assets.*

Top management support cuts across various aspects of the organisation and the implementation phases, as widely confirmed in the literature (Chatterjee 2019; Kikwasi 2018). Organisations are functioning in a competitive, complex environment and dynamic conditions. CSRM is one of Top management's topmost concerns in most organisations to meet the challenges of surviving amid competition. Top management involvement, efforts and support for CSRM includes early acknowledgement and intervention of the people and organisational factors in defining and implementing CSRM policies and all other necessary supports for implementation success (Yaraghi and Langhe 2011). All the participants' affirmations support other studies that top management support is critical for CSRM implementation success.
P7 commented:

> *One of the most critical success factors that contributed to the success of CSRM in our organisation* ***is commitment*** *and* ***support from top management****; without their* ***suppor****t to introduce a CSRM implementation program, the implementation of CSRM would never have come through.*

Von Solms and Van Niekerk (2013) highlighted the role of human (people factor) in CS; Top management's conviction of CSRM implementation's importance leads to approval of sufficient budgets and enforcement of policies and processes controls to gain employees commitment and compliance. This further sets the tone that in implementing CSRM policies, employee engagement through awareness and training is directly proportional to enhancing an operational cyber risk-free organisation (Hadlington 2017; Siponen, Mahmood and Pahnila 2014).

- **Awareness**

Awareness in this study context is conceptualised in section 2.7.2. Awareness also goes a step further in understanding the leadership team's risk management process implementation. Thus,

awareness helps people (all stakeholders) recognise CS risks and threats and respond appropriately to mitigate them. Ultimately, awareness plays a vital role in CSRM implementation success.

Data analysis of participants from case study A shows that people's involvement through effective communication of awareness education programmes in CSRM implementation plays a significant role. It allows the staff to buy in, manage resistances, practice risk mitigation plans and CSRM implementation processes. P1 stated that:

> *The goal of **awareness** programmes is to inform stakeholders **of CS risks** and threats and make sense of the organisation's progress towards dangers of ignorance of these risks, countermeasures and impacts of using different mitigation strategies.*

More importantly, P6 added that:

> ***Awareness training** provides opportunities for stakeholders to understand and reduce ambiguities regarding their roles and responsibilities as the organisation's structure changes and seeks necessary clarifications.*

Awareness initiatives are continuous programmes through various mediums, including nuggets on cyber threats and countermeasures, newsletters sent via emails to users once in the month, bulletin boards, web posters and short videos. One of the most effective means of mitigating user negligence and soliciting employee compliance is employees engagement in security policies through interaction at risk workshops (Mikes and Kaplan 2014). With enthusiasm, P7 stated that one of the creative awareness initiatives during face-face awareness classroom and video training in case study A is:

> *Allow employees to be the risk owners-this requires getting a little more creative and personal with CS awareness training.*

Measures of awareness programmes and education's effectiveness strengthen transaction security and reduce CSRM implementation deficiencies. The CISO explained that:

Before implementing CSRM and awareness training, most employees consider CS a technology issue, i.e., IT staff issues.

Furthermore, the enterprise security manager added:

Sending and receiving of mails are not properly managed to avoid any cyber threat or attacks like phishing and the use of USB. Hence, the percentage of the organisation's cyber-attack-related events measures the effectiveness of awareness initiatives and programmes.

Sequel to the initiation of the CSRM implementation in the company, all participants explained that the organisation witnessed significant top-down buy-in, improvement and cooperation from everyone at all levels. For example, the CISO said:

CS awareness helps shape this expectation and imbibe in everyone that CS problem is everyone's problem.

There is a strong probability that 95% of CS breaches are due to inadvertent human error and insider threats. CS awareness and education among employees can reduce enterprise CS risks and costs. Also, the CISO elaborated that:

*CS awareness training helps **inform** stakeholders of the human frailties and **alerts** people with potential insider threat tendencies because they cannot get away with such activities but are prosecuted before they foolishly compromise the environment. Raises **awareness** of data sensitivity on systems and ensures the subsequent procedures are correct. Finally, **equip** staff with proper tactics to avoid phishing and other related vices to reduce data breaches.*

Corroborating awareness education's effectiveness as an important success factor for CSRM implementation in line with the literature, five participants also confirmed the 13 values gained from awareness programmes. These include: The increased capability to reduce phishing and data breaches because employees can now identify phishing emails/links and report more frequently suspicious mails; Flash drives seen around the office environment are brought for proper checks; Emails are forwarded to the security team for analysis by staff before opening unsure web links; Reduced uncertainties regarding roles and responsibilities expectations of staff towards CSRM;

Education of staff and users on CS risks and threats landscape; Ensures strict adherence to CSRM policies and procedures; Reduction in the number of broken controls and risk exposures; Improves organisations risk culture; Reduction in the enterprise security risk costs and financial loss.

- **Training**

Training is a formal learning process focusing on acquiring the necessary physical skills to perform CSRM tasks, processes, and procedures with minimal effort to achieve CSRM implementation goals and business objectives. Active top management involvement motivates all stakeholders to fight the all-out cyberwar through knowledge acquisition, adequate technical know-how, necessary skills, responsible behaviours in handling and using appropriate technology and many more.

Many experts contend that humans constitute both the strongest and weakest links in the CS chains. The CSRM implementation and business challenges require efficient management and behavioural care management because people, not technology, process (identify, assess and act) information. People have become a central part of all the support systems as assets (just as data and technology), threats and vulnerability (Harrison and Jürjens 2017).

Training and awareness of stakeholders are inevitable and directly proportional to enhancing a CSRM implementation success that paves the way for an operational, cyber risk–free organisation. Many organisations provide several types of training to their stakeholders, more often to direct employees. While some engage in a formal in-house training process, others employ external consultants for training employees using different methods.

Awareness and training programmes ranked first among the factors for CSRM implementation success in case study A. Cybersecurity risk management awareness and training programmes constitute part of the policies signed and read by all new employees as a significant part of the boarding process for new entrants. The CISO added that:

> *Policies, procedures, or counter-measure training programmes form part of the company's living documents. These documents undergo quarterly review and updates, and those updates are appropriately communicated. We have an Electronic Document Management System (EDMS) platform that hosts these documents, reviewed, and scored by respective employees.*

Face-face classroom instructor-led company-wide training medium is not frequent due to time constraints in organising such training. Other digital training media include subscriptions with Udemy (a real-time training and learning platform for employees to learn key skills about organisational challenges). All staff can partake in CSRM training via their laptops anywhere and anytime. A user logging and audit trail are employed to review incidents before and after CS training measures such as training's effectiveness. Also, the enterprise security manager stated that:

> *We have a balanced scorecard report integrated into our Security Information and Event Monitoring (SIEM) platform to review significant occurrences, that is, CS risk exposures based on a specific time of the year and how to mitigate the risks.*

Based on internal audits, continuous improvement reports reported non-conformities about user interactions are monitored and compared with results before and after a major CS training. The data security team frequently sends quizzes to all staff to measure CSRM training benefits. More importantly, any staff who fails the training as part of the organisation's onboarding process will not join the organisation.

The benefits of training include educating staff on the new cyber threats landscape, raising awareness of data sensitivity, ensuring that procedures are correctly followed and equipping staff with proper tactics to avoid phishing and other related vices to reduce data breaches. The information security specialist highlighted that:

> ***CSRM capability*** *(staff and business partners) through* ***awareness training*** *has helped* ***establish trust*** *and* ***grow the business*** *because of the significant reduction in* ***CSRM deficiencies.*** *The stakeholders know that their data is protected.*

Cybersecurity risk management implementation needs transcend technical expertise or professionals or an IT issue. The pathway to CSRM implementation success necessitates CSRM practices and controls with mitigating user negligence through effective training and necessary tools instead of a checklist of dos and don’ts (Kennedy 2016).

It shows that people factors through awareness and training programmes and top management support induce **employee engagement** with CSRM security policies and implementation processes. The ceaseless brief but vital employee engagement is identified as a sub-theme within

the people factor if CSRM implementation success is achieved in the organisation. The CISO emphasised the need for employee engagement:

> *We are majorly dealing with weaponised codes broadcasted across the internet to mutate and self-replicate. For CSRM to be successful, employee engagement is one must-approach from a multidimensional perspective.*

5.3.2.3 Technology Factors

In this study, the theme, Technology factors, refers to tools and resources (hardware and software, tangible and intangible), risk identification and analysis tools and techniques used in carrying out CSRM work activities. All the participants emphasised the importance of technology. Technology mediates between task (process), people and organisational factors to transform inputs into outputs. The availability and optimal use of technology factors to CSRM implementation success. The identified sub-themes include IT competence and System Quality. Figure 5.3 shows the NVivo representation of the theme and sub-themes.

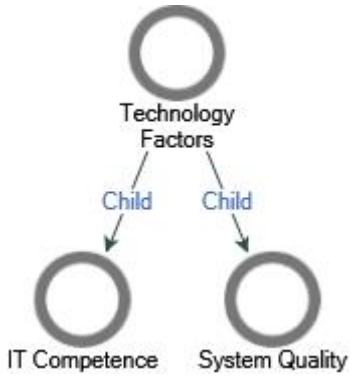

Figure 5.3: Technology Factors Sub-Theme for CSRM Implementation Success

The detailed discussion of the themes is as follow:

- **IT Competence**

IT competence is conceptualised as the combined and interrelated capabilities of technological resources to consistently fulfil its business objective. Information technology/systems continue to evolve and interconnect businesses to increase access to information, data, decentralisation of

business processes, numerous CS issues and solutions. In CSRM implementation success, adequately equipping employees with the relevant skills set for unique managerial or departmental positions is important. Technical control thus becomes a significant part of CSRM implementation for organisational performance and success. In line with previous studies that CS risk is becoming more sophisticated and seems inevitable in business, in-depth knowledge of information technology, information systems, and risk management is essential (Hoffmann, Kiedrowicz and Stanik 2016; Webb et al. 2014).

Awareness education and training programs ensure that stakeholders increase knowledge, confidence, expertise, and competence with IT and IT systems for CSRM. IT competence entails using new technology systems, understanding and integrating the new processes and controls within the CSRM system. Hence, the need to highlight the interrelationship between various factors within the CSRM implementation success framework. That is, how the work of the employees influences one another.

IT competence is a factor that plays a vital role in CSRM implementation success as the enhancement of IT competencies positively affects and strengthen CSRM for a sustainable competitive advantage and organisational performance (Spears and Barki 2010). Expert skills and knowledge are required to understand, deploy, and use information technologies for CS/information security practice. Various technical solutions have been developed for CSRM. Highlighting the inextricable links between humans and technology as key success factors in CSRM implementation, the CISO, with 20 years of experience, commented:

> *The primary concept in achieving a risk-based CS management system revolves around* ***People, Process and Technology*** *(*Highlighted for emphasis based on the conversation tone). *Technical control is a significant part of CSRM implementation. The IT team can deploy systems through internal and outsourced resources to deploy encryption, antivirus software, Intrusion Detection Systems (IDSs), firewalls and the principle of least privilege*.

The process of threat identification, assessment and deployment and implementation of necessary controls and mitigation activities require competent teams. In case study A, the IT capability of staff, both inbound and outsourced, helped achieve CSRM implementation success. The head of enterprise security reported that:

*The **IT team** consists of **subject experts** in all areas with many **skillsets**.*

The statement means that dedicated technology experts are the primary users and implementers of CSRM in case study A with technical controls as a safety net peradventure employees make any mistake. Knowing that CSRM is not just an IT staff issue, the strict penalty measure ensures end-users of IT systems follow a sound process and enforce compliance with operational procedures. In contrast, in case study A, the security teams enforce compliance with policies and processes through technical controls through their IT competence. The CISO reiterated:

> *We do not measure whether end-user follow sound CSRM operation processes but enforce them with technical controls. Microsoft Enterprise Mobility Suite (EMS+Security) is one product that helps control user interactions with the enterprise.*

According to section 5.3.1, management allocates an appropriate budget for technical resources and human resource training. This aligns with literature that availability of knowledge bases improves the use of technology and people's contextual understandings and skills to operate, use or adapt appropriate technology to achieve value-creation processes for CSRM implementation success (Bednar and Welch 2019). Therefore, the IT staff are competent in using the right technology to improve task accomplishment by better controlling the variations in optimising the technological system across the organisation to achieve CSRM implementation success.

- **System Quality**

The quality of the CSRM system is an important factor for CSRM implementation success. In this study context, system quality refers to the technology's availability and reliability for CSRM implementation tasks (Palvia, Sharma and Conrath 2001). In line with the use of technology controls above, if the system's quality does not measure up to standard, it will be highly challenging to achieve the set goals and objectives of implementing CSRM.

Various tools and techniques are used for CSRM implementation. Case study A, being an E-retail organisation, information security of the TRIAD (confidentiality, integrity, and availability) is of utmost importance. Confidentiality of sensitive data means information protection of sensitive data everywhere, in motion and when shared—restricting and gaining visibility and control over the files used with a comprehensive and integrated information protection solution. The integrity

of the systems entails identity and access management by controlling who can write, change, or delete data. This allows secure connections between people, devices, apps, and data. Availability means ensuring that systems are up and running when they are needed.

The list of available systems for CSRM in case study A is exhaustive, but the participants mentioned important ones, namely:

- **Access technical control tools**: Microsoft Enterprise Mobility Suite (EMS+Security): helps control user interactions with the enterprise, encryption, antivirus software, Intrusion Detection Systems (IDSs) and firewalls.
- **Transactions and authentications tools**: multifactor authentication: a security layer that helps protect against a data breach through compromised credentials. It requires authentication from independent categories of authentications to verify users' identities for login or transactions. Two-step verification is Risk-Based conditional access based on profile enforcement with two things already known to the organisation. So also, Application access only through managed Apps.
- **Lightweight Directory Access Protocol (LDAP):** is a software protocol that enables individuals, staff, or anyone to locate resources such as files and devices in the organisation's corporate intranet or the public Internet.
- **Threat protection:** case study A uses adaptive, built-in intelligence to detect and investigate advanced threats, compromised identities and malicious actions across on-premises and cloud environments. Security Information and Event Monitoring (SIEM) software help give a holistic view and correlate security incidences and events across all platforms in real-time. Also, periodic conduct of penetration tests proactively identifies risks and loopholes in the system. Infrastructures to help manage end-point securities include premises servers, cloud servers, databases, source code repository and more.

These technologies mentioned are vital in protecting the numerous organisational vulnerabilities and endpoints. Technological solutions allow the organisation to handle user rights management, identity management, device and application management and end-point protection. Staff can securely access company data, applications, and software from virtually anywhere at any point in time.

The quality of the technology system for performing risk management tasks in case study A was well-proven and reliable, compliant with industry-standard to ensure and exploit the benefits of

CSRM, giving rise to their competitive edge. In CSRM, the system's quality is associated with its functionalities and performance regarding CSRM implementation. The dynamic interface of enablement and support of technology's quality for implementing CSRM tasks and processes makes it essential for a successful operation. The cost of technology and lack of adequate knowledge or business case to invest in risk management are significant challenges that affect the use of technology for risk management (Lee and Green 2015). Most interviewees emphasised technical control: technological resources' availability and maximum benefit as a significant part of the CSRM implementation success factor.

In line with previous studies, non-standard technologies impact the use of technology for risk management. The availability of reliable, proven technologies and tools improves covering all risk management tasks (Lyytinen and Newman 2008).

5.3.2.4 Process Factors

Risk management is a process-based framework that assists in managing CS in organisations. CSRM is an emerging domain for which expert knowledge of the process and dedicated resources are necessary. Quality technology alone will not suffice for reducing human vulnerabilities, but a combination of technology, people and processes must achieve a successful CSRM implementation.

Therefore, organisations equipped with the appropriate security technology, armed people with knowledge and documented processes can successfully implement risk management processes to defend against most threats. The process factors refer to the process of risk management and controls for managing CSRM implementation success. The identified sub-themes include Risk management, CSRM policies and Security Audit.

- **Risk Management**

The risk management process is defined in this study context in section 2.4.2. There are broad perspectives and various international agreements on the necessary elements for a CSRM process (section 2.4.2). This accounts for a growing range of frameworks, applicable body of knowledge, capable methodologies, tools and techniques and vast experience of practical implementation of CSRM across many organisations.

Case study A, an e-retail organisation that prioritises information security, adopts the following three significant frameworks and standards to develop its in-built framework and ISO 37001 for CS passively:

- Payment Card Industry Data Security Standard (PCI-DSS)- is regulated by the Payment Card Industry (PCI) Council for all organisations that store, process, or transit Card Holder information.
- National Institute for Standard and Technology (NIST) - a comprehensive framework that helps develop robust security strategy with high consideration for critical tasks/processes such as risk management, incidence response, training, and awareness.
- Information Security Management Standard (ISO27001) - for managing information security within any size of the organisation. The Risk Management components part of the standard help address risk around the people, technology, and processes. It follows some internal policies for the cyber/information security risk assessment process to focus on critical areas of concern and prioritise its use of resources to maximise response and recovery efforts.

In the words of P2:

> *We have implemented many standards such as ISO27001, ISO 37001 and PCI-DSS to protect our information assets but follow ISO 27001 mostly. Although risk management is tedious, the key phases include risk assessment and mitigation. The IT and risk management teams work together to achieve the CSRM implementation objectives.*

All the participants commend their CSRM implementation success to strict adherence to risk management standards. Head, enterprise security asserted that:

> *The CISO and Security Engineers are experts in their fields and treat the standards, for example, ISO 27001, as a 'Bible'.*

Furthermore, the CISO explained that:

> *Any cyber/information security risk assessment is how an organisation focuses on critical areas of concern and prioritises its use of resources to maximise response and recovery efforts.*

The adoption and use of these frameworks confirm the team's in-depth CSRM knowledge in case study A. The risk assessment evaluates existing technical, operational and management controls against threats to assets, processes, and information systems. The organisation's systems are categorised, identifying the systems and resources. The assessment comprises 7 stage processes, namely: (a) Definition of assessment scope; (b) identification of threat sources and events; (c) identification of vulnerabilities to the threats identified through media such as questionnaires, scans, interviews (d) determination of likelihood of threats occurrence and degree of vulnerability to those threats (high, medium or low); (e) impacts of the loss of confidentiality, integrity or availability of asset could have on the organisation; (f) Risk analysis (examines the threats, vulnerabilities, the likelihood that the threat will take place and the impact of it should it occur based on a 3-point-scale. The 3-point scale for the likelihood ranges from 1=improbable, 2 = likely to 3=almost certain; the 3-point scale for the impact ranges from 1=negligible, 2=moderate to 3=high to form the risk matrix by multiplying the likelihood with the impact; (g) Finally, the treatment plan based on the risk analysis through the incorporation of controls to mitigate risks.

Risk treatment options of identified unacceptable risks include:

1) Application of appropriate controls to reduce the likelihood and or impact of the risk.
2) Avoid risk by taking necessary actions to mitigate it.
3) Risk Transfer to another third-party insurer or supplier.

Monitoring and evaluation control processes are Security Incident and Event Management (SIEM) software which gives complete visibility of what is happening on the organisation's network. SIEM helps the IT teams be more proactive in managing security threats by analysing the event and log data in real-time to provide event correlation, threat monitoring and incident response. The security team's incidence management response plans are the first line of response for any security incidence depending on the issue's scale. Continuity plans form an effective contingency plan in monitoring and continuous improvement, backed by awareness training for new and old staff and regular penetration tests against the system. The risk manager confirmed that:

> *The risk management method discussed and shared has proven effective because we have not recorded any CS breaches in the last five years.*

The risk management processes showed a bedrock for effective CSRM implementation performance. They targeted proactive solutions that focused on critical areas of concern and prioritised its use of resources to maximize response and recovery efforts for business continuity.

- **CSRM Policies**

Cyber security policies are an essential success factor in ensuring all the employees are involved in securing the organisation's assets and significantly reducing errors. These policies are high-level documents that consist of regulations and directions that must be followed by all employees in the organisation as required and prescribed by the chosen security risk management standards. CSRM policies clarify and define the CSRM objectives and specify employees' corresponding responsibilities towards achieving these objectives (Ma, Johnston and Pearson 2008). It is pertinent that the policies must clearly understand and communicate CSRM objectives and the responsibilities of all the stakeholders and employees involved. The policies are often reviewed regularly to meet the current organisational needs.

In case study A, designed policies are to enforce workflows and processes. The CISO highlighted that:

> *CSRM policies also include technical controls to ensure that processes, procedures, and workflows are strictly enforced, with or without proper supervision, despite continuously attempted breaches – none successfully penetrated yet.*

The **enforcement of security policies** aligned with the CSRM and business goals and objectives necessitates awareness and training on security policies and the implementation of technical controls, processes, and procedures. Compliance with security policies is an enhanced control to reduce breaches and successful cyber-attacks. The respondents' acclaim that the CS policies are too many to mention as required by the adopted security frameworks and standards but have been very effective in CSRM implementation success. These policies form part of the organisation's living documents, which all employees must read and sign as part of the onboarding process.

The above assertions by all the participants confirm that the design and enforcement of policies are key success factors for CSRM implementation success in line with existing literature (Al-Awadi and Renaud 2007). A few such policies relevant to CSRM success are email acceptable use policy, Bring Your Own Device (BYOD), Clear Screen Policy, Information Security policy

and Multi-Factor Authentication (MFA). Employee engagement and adherence to CS policies enhance a risk-free cyber organisation (Siponen, Mahmood and Pahnila 2014).

- **Security Audit**

The previous sections discussed that security policies ensure CSRM implementation success. CSRM policies comprise rules, processes, and procedures set out as security controls to comply with specific CSRM standards or frameworks. This study conceptualises monitoring, evaluating, measuring, and reporting compliance with these security controls as a **security audit**. The participants unanimously agree that a security audit has been critical for CSRM implementation success.

Since a CS audit's objective is to provide management with an assessment of an organisation's CS policies and procedures and their operating effectiveness, P7 commented:

> *Cybersecurity audit effectiveness on CSRM implementation is **VERY HIGH.***

Likewise, the risk manager explained:

> *A security audit is critical in implementing the effectiveness of the controls, processes, and policies, without which there will not be a maker or checker.*

These assertions from case study A align with the literature that security audits discover gaps in the CSRM implementation process and check **CSRM maturity levels** in an organisation. Thus, the security audit positively influences CSRM implementation's success and shows the interrelationship between the socio-technical factors (Islam, Farah and Stafford 2018; Kahyaoglu and Caliyurt 2018). In the words of the CISO:

> *We continually improve by monitoring regular improvement reports based on our internal audits such as awareness & training effectiveness, process controls, and data management designs and protections, leading to our record's overall success.*

5.3.2.5 Organisational Factors

The organisational factors align the CSRM strategy with the overarching organisational strategy and specific business needs for CSRM implementation success. The sub-themes that emerged are Business alignment with CSRM goals, corporate governance, and adequate budget planning.

- **Business Alignment with CSRM Goals**

A strategically focused or business-driven CSRM implementation strategy is vital in aligning business goals with CSRM goals to be successful (Spears and Barki 2010; Tu et al. 2018). Participants from Case study A confirmed that business alignment with CSRM goals is a critical success factor in CSRM implementation. Their business goals, objectives, values, and needs directly depend on the fundamental organisational goals. In setting the business objectives, the business processes are evaluated, and CSRM policies and procedures are developed to achieve the business objectives. Here are some of how the alignment of business goals with CSRM enhance CSRM implementation success. The risk manager supported that:

> ***CSRM objectives cannot*** *be separated from the* ***organisational goals and objectives****.*
> *CSRM objectives* ***must align*** *with the corporate objectives to be successful.* ***Deviation from this is a recipe for failure****.*

Most CSRM policy objectives, including technical controls, are aligned with, or driven by business requirements and designed to enforce workflows and processes to achieve CSRM implementation success. When organisational strategies align with security strategies, maximum success is achievable by putting people (assign roles and responsibilities), procedures and policies in place. The CISO supported this with the following approaches:

> *The first approach is to define roles and responsibilities. Then capture the business process and develop policies and procedures aligned with the business objective.*

These findings confirm that the technical staff, middle management, and risk management staff believe that the organisation designed CSRM goals to align with business goals to achieve CSRM implementation success and not just for security sake. Furthermore, the analysis from the data security officer explains the effectiveness of the alignment of business goals with CSRM goals in ensuring CSRM implementation success as follows:

a) Increase in the operational use of information technology and internet activities by customers.
b) Increased financial profit margin because computer servers are safe from security threats and malware.

These affirmations support the literature that the business alignment with CSRM goals helps create a formal CSRM implementation structure. At various levels within the organisation, the managers and users are more responsible and willing to support sound CSRM implementation practices. Thus, Business alignment with CSRM goals is a success factor for CSRM implementation.

- **Corporate Governance**

In this research, corporate governance is defined as the set of responsibilities and practices exercised by the board and executive management to provide strategic direction, achieve objectives, and ascertain efficient CSRM implementations through the appropriate and verifiable responsible use of organisational resources.

Corporate governance and risk management are interrelated and interdependent (Allen et al. 2018). The participants confirmed corporate governance as a necessary factor for CSRM implementation success. There is a top-down model in which roles and responsibilities are assigned to support all strategic decisions for CSRM implementation success. P1 explained:

> *Our organisation follows a **Plan-Do-Check-Act (PDCA) model** where the **senior management** remains the **project owners** and a top-down model to drive sound governance principles. The PDCA framework **supports risk-based decision making** and **oversight across all organisation operations** to identify, assess, manage, and communicate risks.*

Corporate governance creates value and establishes an organisational structure that helps set appropriate plans and methodology for ensuring effective CSRM implementation success and business survival. Integrating a risk management initiative as one of the vital parts of the corporate governance code in many countries ensures that enterprise CSRM is effectively implemented (Manab, Kassim and Hussin 2010). The data security analyst responded that:

> *We now have best-practice action plans, risk assessment and management and compliance solutions focusing on cyber resilience/security, data protection and business continuity with corporate governance.*

By clarifying essential roles and duties through corporate governance to enhance an efficient way of communicating risk management and controls, risk management initiative's success is assured irrespective of the organisational size and complexity (Institute of Internal Auditors 2013).
P4 and P2 explained that:

> *Because various individuals **have specific roles**, setting methodologies and procedures aligned with the organisation's standard policy has improved CSRM success (P4).*

> ***A dedicated team of CISO, Risk Manager, Security Engineers and the legal manager** must ensure the organisation achieve its business and security goals and objectives. These **governance teams** are experts in their various fields*.

Case study A agrees with the literature that corporate governance is a critical component of CSRM implementation success that defines the structure, strategy, and methodology for CSRM implementation plans to identify, assess, monitor, and mitigate organisational CS risks (Dhillon, Tejay and Hong 2007).

- **Adequate Budget**

This study conceptualised adequate budget planning as having sufficient financial support to meet both the human capital resource needs and CSRM implementation activities and operations. The overall response to adequate budget planning agrees that management supported achieving CSRM implementation goals, and success is unsurprising.
The information security specialist from Case study A comments that:

> *Since we were able to convince the management of the importance of CS in the organisation, **investment in CSRM implementation** has become the **topmost priority** since any vulnerability in the system can substantially negatively impact the organisation.*

Adequate budget planning creates enormous value for the organisation in various ways, namely:

- Risk assessment and procurement of necessary mitigation tools and actions.
- Assets and brand protection.
- High-level engagement with the partners, associates, and clients.
- Fulfilling customer expectations and building trust.

The data officer sums it up in his response:

> *An **investment in CSRM creates value** for the organisation in addressing risks like asset protection, IT security, cyber terrorism, and crime.*

The above statement supports the literature that decision-makers must compare the opportunity cost of a breach over all other costs and prioritise adequate budget planning as an informed decision for CSRM implementation success (Al-Awadi and Renaud 2007). Adequate investment planning is thus a success factor for CSRM implementation success (Tu et al. 2018).

5.3.2.6 Evaluation of Factors for CSRM Implementation Success in Case Study A

The participants were asked about the overview of the factors identified. Analysis of the review revealed that participants agree that all the factors are success factors for CSRM implementation. Figure 5.4 shows a matrix coding of the overview of the factors.

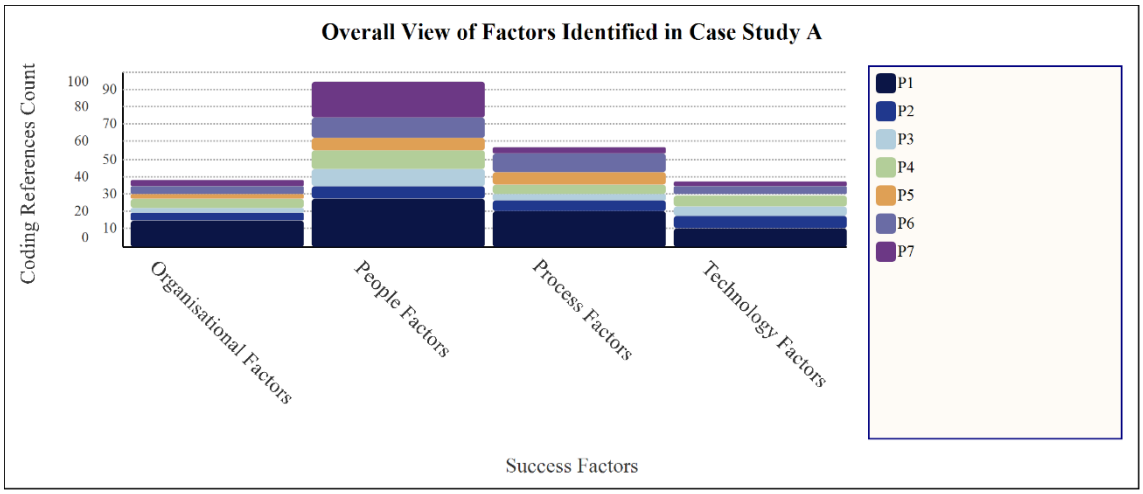

Figure 5.4: Overall View of Factors Identified in Case Study A

Figure 5.4 above shows that about 95% of the participants prioritise people factors as the key critical success factors among the major four dimensions, while Technological factors ranked lowest (about 40%). Studies have identified a lack of appropriate risk behaviours and adequate knowledge, learning, training as implementation challenges to any risk management approach (Siponen, Mahmood and Pahnila 2014).

These suggest that CSRM implementation's effectiveness eventually depends on people who identify, analyse and coordinate risk management processes, not the technology, frameworks, or policies. This further explains the need for employee engagement in policies and decision making regarding CSRM implementation (Chabinsky 2014). Furthermore, compared the sub-factors for the people factors, as shown in Figure 5.5 below.

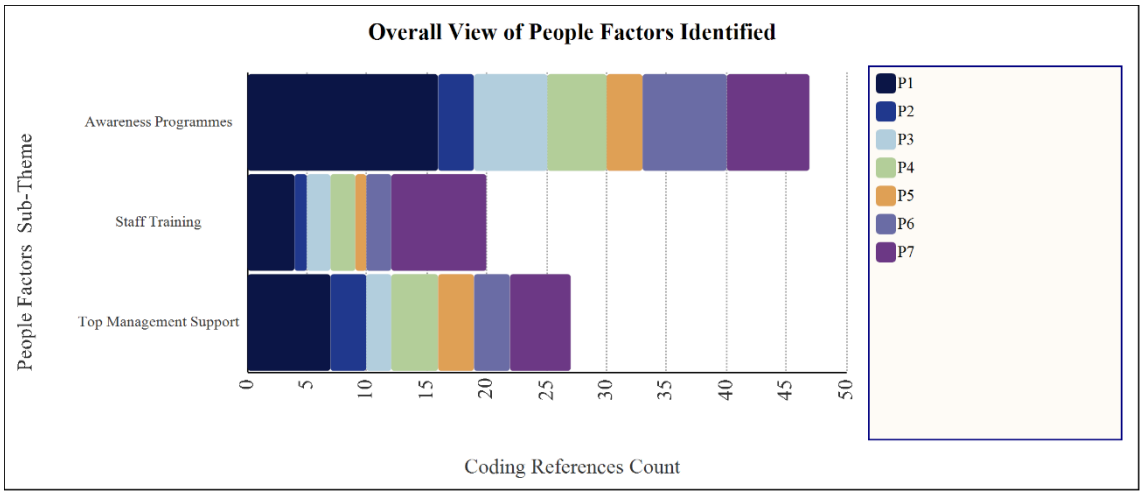

Figure 5.5: Overall View of People Factors Identified

Kennedy (2016) draws attention to a lack of awareness and training and training without risk workshops, not applying to the Keep It Silly Simple (KISS) mindset among the recurrent implementation challenges in major studies. Figure 5.5 corroborates the importance of awareness education as a critical success factor for CSRM implementation success followed by top management support. Some evaluation measures of the relationship between the factors and CSRM implementation success are the effectiveness of the factor, its value creation or derived benefits on the implementation success and the organisation. Figure 5.6 reveals the values derived from the effectiveness of awareness and training sub-theme.

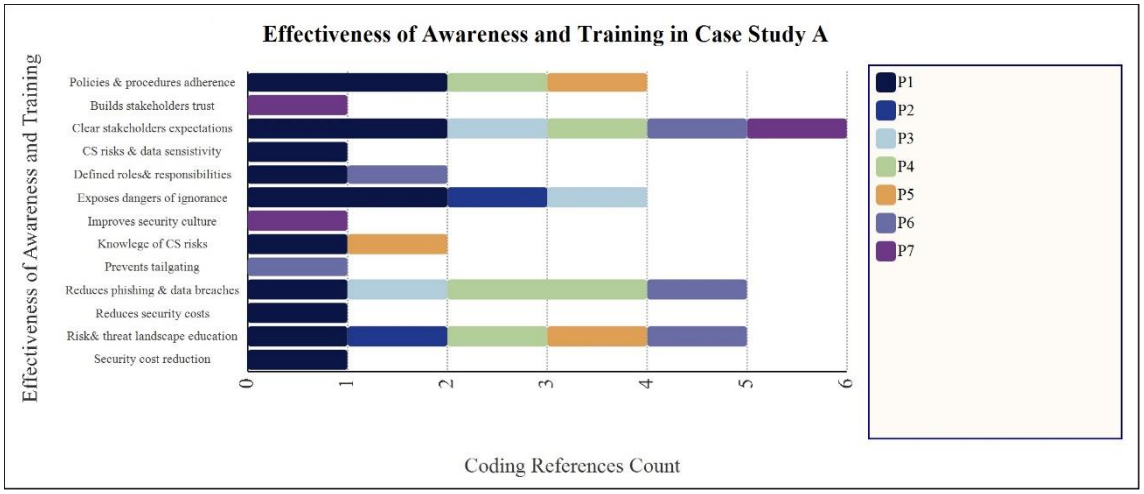

Figure 5.6: Effectiveness of Awareness and Training Factors Identified in Case Study A

Figure 5.6 shows that awareness and training led to staff education on the risk and threat landscape, which reduces uncertainties regarding CS expectations, roles, and responsibilities. Thereby increasing employees' capability to reduce phishing and data breaches and reduce financial losses due to security breaches in the organisation.
The risk manager stated that:

> *In recent times, we have not experienced CS-related issues. CSRM awareness and training are not taken lightly by the security governance team, so the staff has a relatively high compliance level.*

While reviewing the overall view of the success factors in the framework for the study, P1 affirms that:

> *Leveraging behavioural controls rather than static rules is a far more effective work tool within their CSRM practices.*

These demonstrate the direct relationship between awareness and training and CSRM implementation success. Therefore, awareness and training are success factors for CSRM implementation. This illustration also highlights the direct relationships between the social and technical factors in achieving CSRM implementation success.

Figure 5.7 shows the effectiveness of top management support on CSRM implementation success. Remarkably, 5 out of the 7 participants correlate CSRM implementation success to top management support.

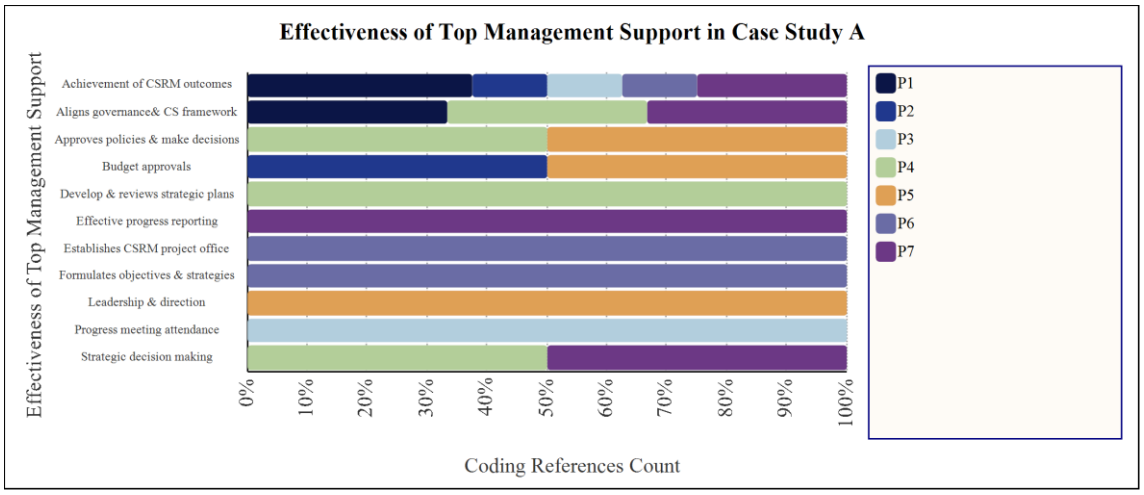

Figure 5.7: Effectiveness of Top Management Support

Figure 5.7 above illustrates that top management provides leadership and direction by aligning the enterprise governance framework with the CS framework through strategic decision-making that ensures the intended CSRM implementation outcome. Consistent with the earlier findings (Chatterjee 2019), top management approves budget planning for human and technical resources (staff education and training, acquiring expert IT teams, and purchasing quality technology systems). Also, top management develops and supports policies, adopt change initiatives and drives CSRM implementation.

For organisational factors, aligning CSRM goals with organisation goals ranked first, followed by adequate budget planning and corporate governance (Figure 5.8).

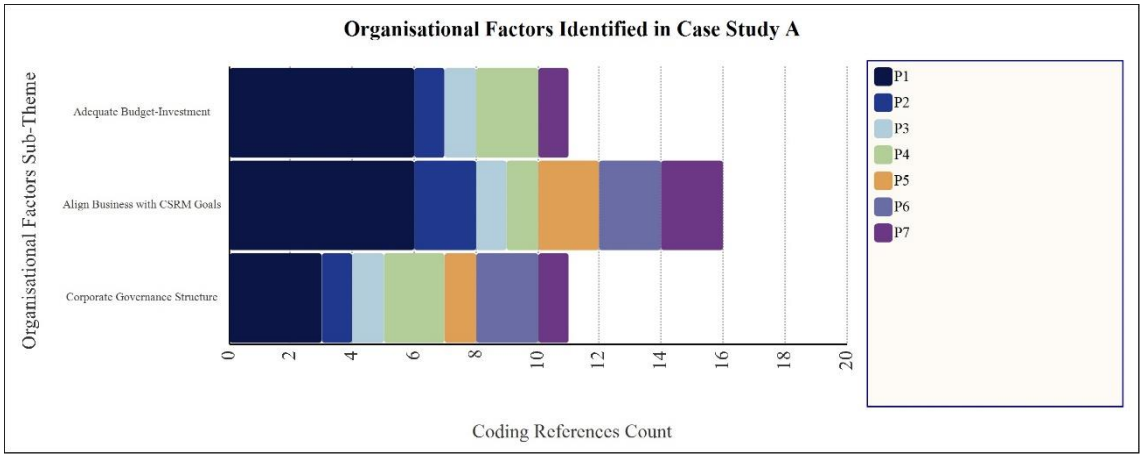

Figure 5.8: Overall View of Organisational Factors Identified

Figure 5.8 above suggests a strong positive relationship between business alignment and adequate budget/investment and corporate governance as success factors for CSRM implementation success. The CISO substantiates this assertion:

> *In ensuring value-added CSRM implementation initiatives, the* ***business strategy*** *must* ***align*** *with the* ***strategic organisational objectives.*** *The* ***enterprise governance*** *must be* ***aligned with the CS governance framework*** *through* ***efficient and effective resource*** *management (****adequate budget planning****,* ***organisation resources*** *and* ***assets****) to achieve the CS implementation program's intended outcomes.*

In the process factors, the need to adopt a risk management approach/standard ranked first, followed by the enforcement of security policies to achieve CSRM implementation success, as illustrated in figure 5.9.

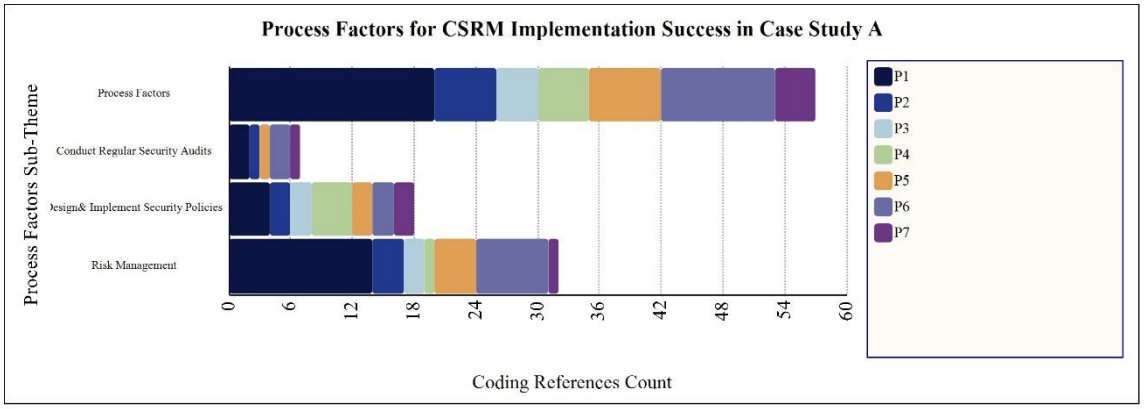

Figure 5.9: Evaluation of Process Factors for CSRM Implementation Success

According to figure 5.9 above, all the participants concur with the literature that adopting a risk management standard is critical to CSRM implementation success. It precedes the design and enforcement of security policies and subsequent audit of compliance with the policies. The standards contain most of the security policies.

Tisdale (2016) posits that the evolving emphasis on risk management emerged as the better strategy and methodology for CSRM. Adopting a risk management standard/framework, understanding and sufficient commitment to the efficient risk management process, setting clear objectives and guidelines for risk management, vulnerability and impact risk identification, risk analysis, treatment and implementing monitoring and reviews systems differentiates an organisation from CSRM failure or success.

During the interview, the participant's views on the identified and discussed factors validate the factors' applicability and grouping. The semi-structured case study approach suggests and recognises that the process of theoretical development could involve some iterations depending on additional insights and new knowledge gained. Some success factors were identified by induction during the interview. The overall response to the review of the factors identified is that all the factors identified were success factors for CSRM implementation in the organisation.
For example, the risk manager and the data security analyst stated that:

> *All the factors are necessary for the successful implementation of CSRM, as discussed (P5).*

> *The discussed factors are essential because, without them, the successful implementation of CSRM would not be possible (P6).*

Although the framework broadly gained merit, some other success factors were suggested (Section 5.3.2.7).
Figure 5.10 shows an overview of the success factors for CSRM implementation.

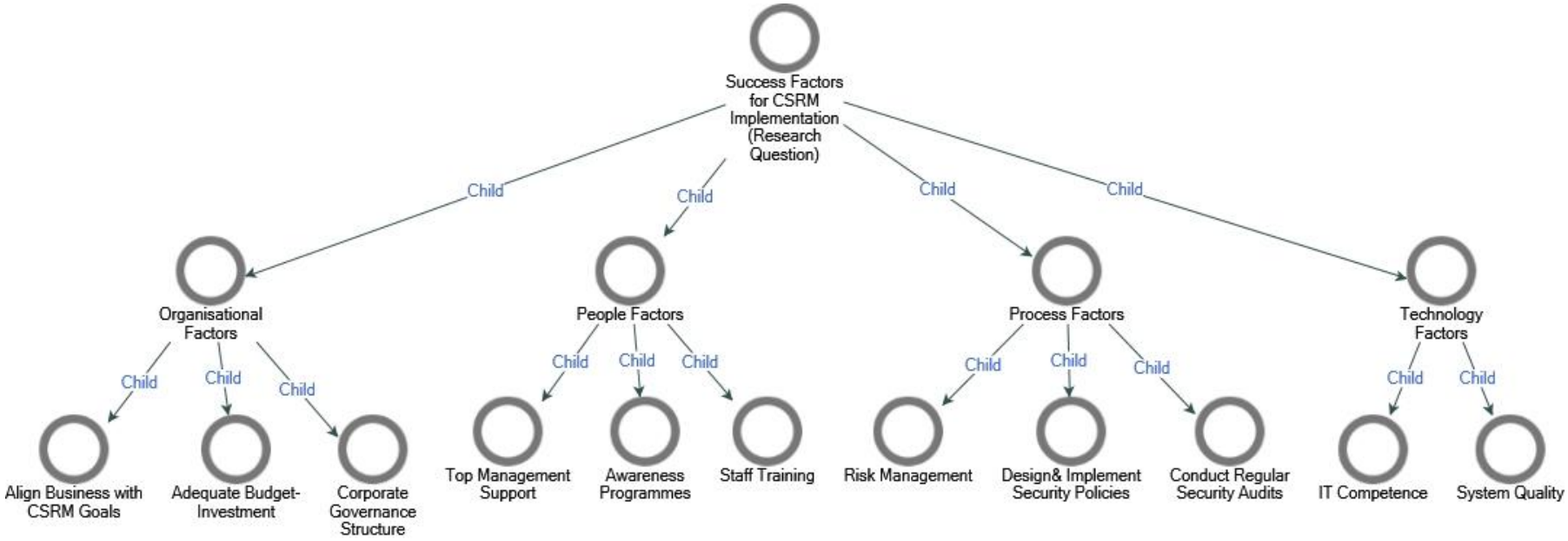

Figure 5.10: Success Factors for CSRM Implementation Success in Case Study A

Finally, figure 5.11 highlights the overall effectiveness or measures of CSRM implementation success in case study A.

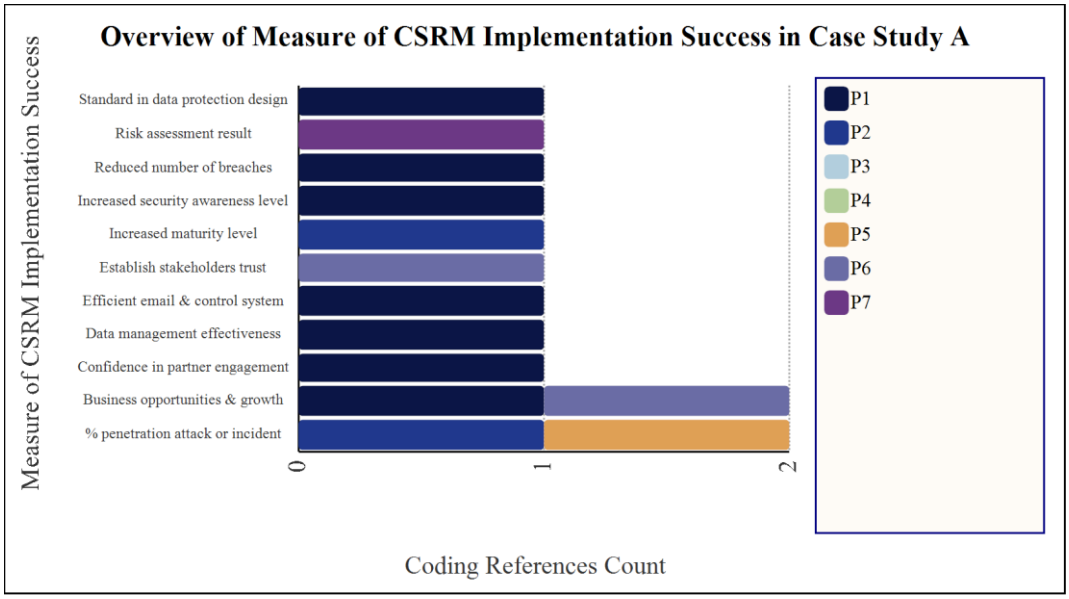

Figure 5.11: Measure of Effectiveness of Case Study A CSRM Implementation Success

Figure 5.11 shows over ten positive results of the effectiveness of CSRM implementation success in case study A. These include an improved level of CSRM maturity using SIX SIGMA[1], creating a standard in data protection design signified by a decrease in the percentage of cyber-attacks and breaches, effective data management, efficient e-mail system and control system resulting from increased workforce awareness of security risk and issues. The establishment of stakeholder's trust leads to tremendous confidence in partner engagement and improved business opportunities. Some other success factors identified are discussed next.

[1] **Six Sigma** is a method that provides organisations tools to improve the capability of their business processes. This increase in performance and decrease in process variation helps lead to deficiencies reduction and improvement in employee morale and quality of products or services and profits.

5.3.2.7 New Success Factors Identified

Five out of seven participants identified new factors during the framework review added to the ones unanimously agreed. Figure 5.12 illustrates the new factors.

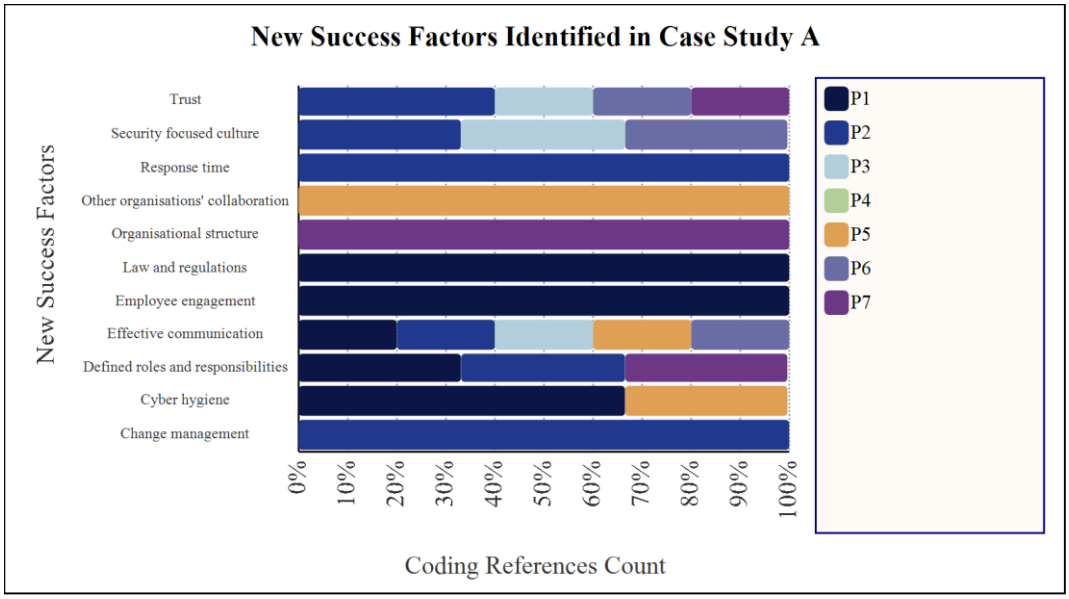

Figure 5.12: New Success Factors Identified

Figure 5.12 highlights the new factors for CSRM implementation factors in case study A. Table 5.5 highlights the identified factors and supportive comments.

Table 5.5: New Factors Identified and Supporting Comments

This item has been removed due to 3rd Party Copyright. The unabridged version of the thesis can be found in the Lanchester Library, Coventry University.

Further literature review substantiates the agreement with these factors (Yaraghi and Langhe 2011).

5.3.2.8 Summary of Case Study A

The summary of the thematic analysis of case A concluded that CSRM implementation was successful based on the proven results of the identified factors' effectiveness. The CSRM centred on identifying systems resources, assessing appropriate controls for the systems and resources and implementing proper controls. The organisation's management has adopted an inclusive approach where all necessary inputs, efforts, and expertise gear towards CSRM implementation success.

The CSRM sums up the process of avoidance than mitigation. Surprisingly, while evaluating the effectiveness and success of CSRM implementation, there were unknown unknowns in case study A. Although the organisation’s CSRM implementation was judged successful, it was done unconsciously from the socio-technical concept perspective but singularly focused on all the broad four dimensions as deemed fit. The organisation was enlightened more on articulating and optimising these factors as success factors.

5.3.3 Introduction to Case Study B

Case study B is a financial services provider that strives to be among the retail bank brand of choice in Nigeria. A respectable bank with a global geographic presence offers its customers a wide range of electronic payment and internet services. Trust remains the bank's key product offering by ensuring confidentiality, integrity, customer data and information availability. Case Study B represented a successful CSRM implementation of an organisation in Nigeria. According to the security risk manager:

> *The overall CSRM implementation success is 70/100.*

In 2018, the bank continued to evaluate, strategise, and overhaul its CS proficiencies to secure its computing practices. Implemented some globally acclaimed CSRM initiatives and practices across its group to predict, detect, identify, protect, prevent, respond, and recover from cyber-attacks across the branches. The selection criteria are consistent innovation towards CSRM implementation across its subsidiaries over two decades of operations with an annual turnover of over 5 billion nairas and an employee size of over 10,000.

The bank’s CSRM implementation focuses on three key operations such as (1) Revamp of existing solutions through the adoption of dependable solutions for increased equipment for 24-hour effectiveness of security operations centre with capabilities of the full depth and breadth visibility of the Group’s IT infrastructure layout and transactional activities across the enterprise. (2) Attracting key skillsets across the globe could drive its strategy through (3) Competency development through staff training and retention to ensure optimal value extraction (Annual report 2018).

Table 5.6 shows the interviewees' profiles at different organisational levels to obtain multiple perceptions about the success factors for CRSM implementation in Case Study B.

Table 5.6: Case Study B Participant's Profile

Participant	Role	Years of Experience
P8	Information Security and Business Continuity	12
P9	Computer Network Engineer	7
P10	CS Risk Manager	8
P11	Security Control and Compliance Manager	8
P12	Data Security Analyst	2
P13	End-User Support Officer	8
P14	Chief Information Security Officer /Lead Implementer	15

Table 5.6 presents the participants with relevant experiences who were willing and able to share their views on the factors contributing to CSRM implementation success in their organisation. Moreover, the participants represent different hierarchical levels and departments with diverse perspectives to increase the validity and reliability of the result. The case study findings for each success factor are discussed in subsequent sections.

5.3.3.1 Success Factors for CSRM Implementation in Case Study B

This section addressed the main research question: What factors influence CSRM implementation success in large organisations in Nigeria. All the participants expressed their views about the factors that lead to successful CSRM implementation. The themes identified by the research questions and the interviewees' responses as sub-themes are coded as parent and child nodes in NVivo outputs, as shown in Table 5.7 below.

Table 5.7: Factors for CSRM Implementation Success Themes and Sub-Themes

Themes (Parent Node)	Sub-Themes (Child Node)
People factors	• Top management support • Awareness • Training
Technology factors	• IT competence • System quality (Task-Technology fit)
Process factors	• Risk management • Enforce CSRM policies • Security audit
Organisational factors	• Business alignment with CSRM goals • Corporate governance • Adequate budget planning

Table 5.7 shows the themes and sub-themes as success factors for CSRM in case study B, comprehensively discussed and analysed.

5.3.3.2 People Factors

Section 2.7.2. conceptualised the People factors theme. CSRM implementation functions of planning, monitoring, reviewing, and improving processes require individuals and teams to succeed. CSRM implementation success depends on people factors as enumerated in section 5.3.2.2 in case study A. The analysis of case study B highlighted the positive impacts of people factors in CSRM implementation success. The identified sub-themes include awareness, training, and top management support. The NVivo representation of the theme and sub-themes (child) is shown in Figure 5.13 below:

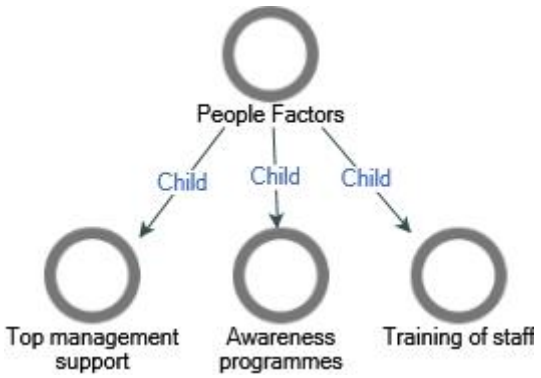

Figure 5.13: People Factors Sub-Theme for CSRM Implementation Success

The sub-themes are discussed in full below.

- **Top Management Support**

Top management support is crucial for CSRM implementation initiatives to succeed because if they do not see the importance of any CSRM programme, none of such initiatives will succeed. Hence, Top management demonstrates their support by ensuring that they are aware of and fully informed of the need for CSRM. In turn, formulate policies, approve the investment, ensure that staff know their security roles and expectations and review risk reports to monitor CSRM implementation success achieved within the organisation.

In case study B, the participants established top management support has been critical for their CSRM implementation success. Resources for CSRM are scarce, so there is a constant balancing act with the necessary and available resources. The CISO explained that:

> *The **initial actions** and **essential process** in CSRM implementation are to get **senior management commitment**; to no small extent **senior management agrees** to the **provision of requirements to execute** CSRM for both **man and material resources.***

While we all know that technology cannot work in isolation and CSRM is everyone's responsibility, the top management often directs the CSRM implementation processes. In the words of the security controls and compliance manager:

> *The **Chief Executive Officer (CEO)** severally remind **all staff** of their **security responsibilities** and attendance at security awareness and training programmes via email. The annual report further highlights the effectiveness of top management support in CSRM implementation success. The CSRM initiatives and successes outline are bold for all customers and the general public to show that **the management supports** the CSRM program.*

All the interviewees' comments further provide evidence supporting prior literature that top management support is critical for implementing CSRM in an organisation (Atoum, Otoom and Abu Ali 2014; Kikwasi 2018).

- **Awareness**

Similar to case study A, section 5.3.2.2 defines awareness in this study context. Awareness is one of the activities closely linked to top management commitment. Thematic analysis of participants' comments from case study B shows a top-down approach to awareness training for enhanced CSRM implementation success. Awareness medium includes weekly flyers, updated intranet portals for staff, multimedia awareness content occasionally within end-users computers and business office screens, simulations and monthly awareness training conducted by the user support staff at each bank branch.

Contrary to expectations, the bank engages in roadshows as a part of awareness programmes to their teaming customers, believing that customers' enlightenment forms an essential aspect of

CSRM implementation success. The awareness programmes also extend to bank customers through emails and text messages alerts. The end user's support officer believes that:

> *The efforts to create awareness for the customers and the bank staff enlightened them on CS.*

The objective of awareness education is to create a cyber-risk-based culture which is a long-term effort, always a struggle in most instances to achieve this feat. Although it is a slow, tedious, and challenging process to change an old mindset, continual management engagement is the best way to achieve results. Participants acknowledged that the management had provided satisfactory awareness to all personnel involved in CSRM implementation and reduced CSRM deficiencies. The lead implementer (CISO) made the point that:

Although adequate awareness is challenging, we have been optimistic about yielding the desired result.

One of the successes of an awareness programme on the CSRM implementation programme is determined by its contribution to strengthening transaction security in the organisation. P10 and P11 demonstrated this**:**

> ***Before** introducing **CSRM awareness**, employees did not know what phishing was, saw no need to password their computers, or had no concern for visitors loitering to have a view of their work systems. **However, within six years of running a CSRM awareness program** in the organisation, affirmatively, **the organisation's security maturity level** has **dramatically increased** (P11).*

> *Mainly **end-users are more conscious of social engineering**. **Awareness** has led to **more reported incidents** and **identified risks by process owners** (P10).*

This agrees with prior literature that the awareness of CSRM is critical in any CSRM approach (Verkerke 2015), particularly in all areas of the implementation phases along the PDCA lifecycle of the CSRM implementation process to produce the required competency (Maarop et al. 2015).

- **Training**

Training is a formal learning process focusing on acquiring the necessary physical skills to perform CSRM tasks, processes, and procedures with minimal effort to achieve CSRM implementation goals and business objectives. The management exemplified support and commitment by providing adequate resources for training for a successful CSRM implementation. Training is critical, particularly for the CSRM implementation team and dedicated employees, to perform their respective tasks and duties.

Further replication of data analysis from the participants in case study B showed that all staff training from the top management to the end-users in CSRM implementation constitutes a core activity within the CSRM implementation framework. For example, P13 observed that:

> *W**hen** we move to Microsoft Office 365**, top executives train internally and externally, enlighten them on the disadvantages of not having perfect CS measures, and gi**ve them simulations.*

Teams assemble at 7.00 am to update them on CS threats and solutions within the organisation technical training for selected roles. This training confirms one reason for the high level of support received from the top management in ensuring CSRM implementation success. Other forms of weekly and monthly training for staff on CS include case studies, computer-based training, and facilitated training at branches. P13 added:

> *Yes, I did a couple of Microsoft and ethical hacking training.*

Interestingly, the bank engages in mystery shopping twice a year for a higher standard of training effectiveness and the management drive to ensure CSRM implementation success. Mystery shopping is when a member of the IT team walks into a branch as a customer asking questions to know how educative the staff are regarding CSRM. Test questions after computer-based training periodic quizzes with prizes are measures for evaluating such training's effectiveness. Furthermore, P13 explains that:

> *The IT team tries to compare and look at the average to get the summary report to see how effective they have been.*

CSRM training has immense benefits in improving stakeholders' capability in CSRM implementation success and its CS maturity level. All the participants established unanimously that the bank's CSRM maturity level has increased in many ways. P11and P13 noted that:

> *The organisation's security is now more mature that staff and users have a security culture embedded in their everyday work (P11).*

> *CS **training is critical in CSRM implementation success and** has been **beneficial** over the years; since joining, we have not had any fraudulent cases or hackers trying to penetrate much into our database (P13).*

The interviewees' findings in case study B have strengthened the conviction that CS training is a critical success factor for CSRM implementation, as found in previous related ISRM studies (Spears and Barki 2010).

5.3.3.3 Technology Factors

Technology factors relate with those defined in Case study A (section 5.3.2.3). Although case study A considers technology factors critical success factors for CSRM implementation, there is tremendous caution concerning case study B. Two out of the participants claim that the significance of technology availability is not a success factor. However, the capability to use security technology is a success factor for CSRM implementation success. The identified theme and sub-themes include IT Competence and System Quality, shown in figure 5.14 below:

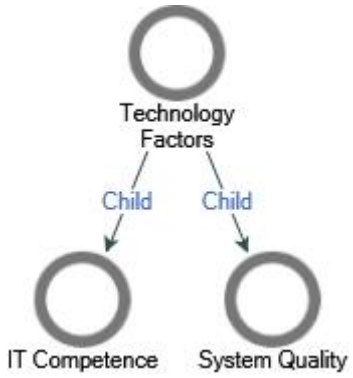

Figure 5.14: Technology Factor Sub-Themes

- **IT Competence**

IT competence is conceptualised in section 5.3.2.3. Previous research highlights that IT competence is a factor that plays a crucial role in CSRM implementation success (Spears and Barki 2010). Skilled personnel with technical expertise must ensure that information technology for CS/information security technologies is gainfully employed and deployed in CSRM implementation practices.

When asked about how staff IT capability, both inbound and outsourced, helped achieve CSRM success in the organisation, the cyber security manager refuted that security will not be embedded without cyber/information security capabilities. However, the ability to enforce technical controls by the IT teams assists in ensuring CSRM implementation success.
For example, P10 stated that:

> *Without monitoring tools to detect, prevent and sanctions violations, they will not comply.*

The above statement agrees with (Caralli et al. 2007) that having a broad array of technology is insufficient as a factor for CSRM. However, technology enables CSRM implementation success by strategically aligning information technology with the organisation's strategic CSRM implementation plan. Innovative and strategic use technology positively affects information technology activities and the organisational CSRM implementation success plan. Thus, IT literacy and competence are success factors for CSRM implementation in the organisation. The result is growth, effective competition in the marketplace and accomplishment of the organisational CSRM implementation goals and objectives.
As P11 states:

> *IT proficiency in using these technologies is vital to achieving CSRM implementation success.*

- **System Quality**

The quality of the CSRM system is an essential factor for CSRM implementation success. In line with the strategic technology use above, CSRM implementation goals are tightly linked to the performance in some key areas and enable high-performance technology.

Case study B use similar tools and techniques with case study A for CSRM implementation. However, using a token and Artificial Intelligence (AI) is an additional tool for access and transactional authentication and protecting the numerous organisational vulnerabilities and endpoints. In corroboration with the previous researcher, Mursu (2002), the technology for performing risk management tasks must be compatible with other software in the organisation. The comments from P10 contradict that:

> ***Technology*** *helps 20%- because technology* ***can only function well*** *when human factors cooperate.*
>
> *However,* ***quality systems*** *have provided* ***more intelligence*** *in* ***identifying vulnerabilities*** *and* ***responding to risk incidents at the endpoint level*** *(P11).*

One of the established key phases of CSRM implementation is identifying threat sources and vulnerabilities within an organisation. Thus, system quality is a success factor for CSRM implementation as more organisations tend towards AI-Driven Security-Aware Defense Mechanism for Advanced Persistent Threats (Li et al. 2019).

5.3.3.4 Process Factors

Risk management is a process-based framework that assists in managing CS in organisations. CSRM is an emerging domain where expert knowledge of the process and dedicated resources are necessary. Managing CS risks successfully in an organisation with a CS programme entails understanding the organisation's inherent risks and implementing a risk management programme together with the strategies to minimise loss and maximize gain (Hopkin 2017; Reza Hosseini et al. 2016). Quality technology alone will not suffice for reducing human vulnerabilities, but a combination of technology, people and processes must achieve a successful CSRM implementation. The process factors comprise the process of risk management and controls for CSRM implementation success. The identified sub-themes include Risk management, CSRM policies and Security Audit.

- **Risk Management**

This study defined the risk management process in section 2.4.2. There are direct relationships between the risk management process and the risk management practices (Kerstin, Simone and

Nicole 2014). Research supports that large organisations, especially financial organisations are average users of cutting-edge risk management practices (Hoyt and Liebenberg 2011; Hudin and Hamid 2014). This is due to the high cost associated with cyber risk management that often hinders the implementation of risk management practices (Fraser 2016). Many authors believe that financial institutions often implement acceptable risk management practices (Paape and Speklè 2012). This confirms that risk management is a key factor for CSRM implementation in large organisations.

A well-managed CSRM program does not add bureaucracy to the process; instead, it helps in most cases to streamline the process and be more effective. Helps to define operational policies and standardize procedures. P8 expressed that in their CS management, the first thing was to conduct a business security risk assessment to understand the organisation's risks before adopting and implementing any controls. The CISO made the point that:

> *A CS risk-managed environment's advantages include improved management processes and corporate risk strategies.*

The organisation claimed not to have witnessed a CS breach in the last five years due to adopting and implementing the ISO 27000 suite components, NIST CS framework, PCI DSS frameworks, and CBN CS framework. These standards provide a holistic framework to build the organisation's CSRM and information asset risk management programme. The lead implementer laid much emphasis on the CBN framework and the ISO 270001:

> *They both cover the majority of the risk spectrum starting from CSRM Scope, Information security policy, Information security risk assessment and process documentation, Information security risk treatment, comprising statements of applicability, Information security risk treatment (Risk treatment process), Information security objectives and plans, competence, operational planning and control, Risk management procedures such as Risk assessment results, Risk treatment results, Metrics, ISMS/security internal audits, ISMS/CS management reviews, Nonconformities and corrective actions.*

The CS risk manager rated the effectiveness of implementing the frameworks' components was rated *90/100* by the CS risk manager over the eight years of experience in CSRM implementation. P11 points out that excellence was achieved because:

The framework provides guidelines on the type of controls that suit the business, and the implemented controls helped reduce our attack surface.

In case study B, the participants' accounts agree with the risk management process applications towards managing risks with potential positive impacts on an organisation (Hudin and Hamid 2014).

- **CSRM Policies**

Cybersecurity policy is a prerequisite for an effective CS programme (Okolo 2016). For a successful CS security risk management implementation, the management formulates policies, ensures policy awareness by all staff, enforces the policies and continuously maintains the policies conformance with the evolving trends of CS risks and the management of such risks (Niemimaa and Niemimaa 2017).

The CSRM programme in case study B exits for over a decade and is very mature. The cyber risk manager explained that:

CSRM policies have been 80% successful in shaping and establishing CSRM culture, enforcing work processes, and enforcing employee compliance.

Business-aligned CSRM depends on how security policies and controls centre on business objectives, needs or values, other than a technology-focused asset (Spears and Barki 2010). Management support with exclusive responsibility for framing, communicating, and executing risk management policies provides a consistent view of the organisation’s CS risks and builds a safety culture. Organisations lacking in placing considerable efforts in training and building employees as a primary way of communicating CS policies are prone to many security breaches and incidents (Siponen, Mahmood and Pahnila 2014; Siponen and Willison 2009).

Cybersecurity policies emphasise the significance of security for the organisation, define CS objectives and specify employees' CSRM responsibility (Ma, Johnston and Pearson 2008). As users become aware of security policies, not necessarily technological approaches, they are much more alert to those that can constitute security challenges and breaches, recognise security incidences, and report more often.

Like case study A, the security policies are too many to recount according to the chosen framework and standards. Examples of applicable policies are acceptable use, vulnerability management, clear desk/screen, password, user management and change management policies. It shows that, to a great extent, the CSRM implementation success trends provide valuable insights and links about the implications of established policies in shaping employees' behaviour (Hu et al. 2012). Thus, the design and enforcement of Security policies are among the success factors for CSRM implementation success in line with extant literature.

- **Security Audit**

The previous section highlights the importance of security policies in CSRM. These policies comprise rules, processes, and procedures set out as security controls in compliance with the chosen CSRM standard or framework. This study conceptualises monitoring, evaluating, measuring and reporting compliance with these security controls as a **security audit**. Some participants agree that a security audit has been a critical success factor for CSRM implementation success. P10 emphasised that:

> ***The audit helps to no small extent in CSRM implementation success*** *with a score of* ***80/100.***

The end-user support officer further explains that there were checks on certain implementations for those deployments to succeed. For example, periodic reports and statistics about the number of breaches had and related audits. These reports help the organisation know if there is a need for improvement.

These assertions from case study B align with the literature that security audit areas need improvements in the CSRM implementation process in an organisation. Thus, the security audit positively influences CSRM implementation's success and shows the interrelationship between the socio-technical factors (Islam, Farah and Stafford 2018; Kahyaoglu and Caliyurt 2018).

5.3.3.5 Organisational Factors

Organisational factors represent the distinctive general features that an organisation exhibits that give it unique characteristics. The organisational factors align the CSRM strategy with the

overarching organisational strategy and specific business needs. The sub-themes that emerged are Business alignment with CSRM goals, Corporate Governance and Adequate Budget Planning.

- **Business Alignment with CSRM Goals**

In this study, aligning business activities and goals with CSRM goals ensures that the organisation strives for a shared CSRM vision and goals. Based on the interviews, it is evident that the alignment of CSRM goals with business goals is an essential aspect of the CSRM implementation process to achieve the overall organisation's vision. In the words of the security controls and the compliance manager, CSRM does not operate in a vacuum. It is part of a business; adequately aligned CSRM brings out the best outcomes and makes all stakeholders see the values.

One of the advantages of a CS risk-managed enterprise-wide framework environment includes enhanced initiatives and decisions that result in improved management processes and integration with corporate risk strategies and organisational objectives. Failure to understand this will undermine the value of a risk management-based approach to CS. P11 added:

> *Broadly, the organisation's CSRM is **in alignment** with **strategic business goals.** This has informed decisions like increased security focus on e-channels like ATM, POS, and others as it moves its customers to those e-channels.*

The participants' comments have shown that identifying CSRM alignment with the organisational business goals is critical for CSRM implementation success. They understand that aligning the CSRM goals with the organisational goals, mission, and objectives have great potential. The alignment helps organisations guide, prioritise, and direct their activities to successfully develop CS strategies implemented in successfully managing security across the organisation. The business management leads and ensures that CS goals and practices align with business objectives and needs (Kayworth and Whitten 2010). Thus, CSRM implementation goals become an enabler of an organisation's strategy instead of a cost centre or burden to the management.

- **Corporate Governance**

Considering the CSRM process after identifying and assessing the highlighted threats and risks, effective management of those risks is paramount. A healthy governance model fitted directly with the CSRM process must be incorporated into its strategic security and organisational goals

outlook. Achievement is when the management is fully persuaded of corporate security risks to mitigate them. When such happens, CSRM correctly implemented and executed ultimately contributes to organisational success and is not a reflective tool (Goss 2017).

This study defines corporate governance as the responsibilities and practices exercised by top management to provide strategic direction and ensure objective achievement while maximising organisational resources to manage CS risks effectively. The appointment of the Chief Risk Officers or CISO or risk champions seen today, especially in most large organisations, is a general but distinctive phenomenon to suggest a shift in thinking towards CSRM implementation success (Fraser 2016). It has now dawned on senior management or serious CSRM conscious organisation to invent some new realm of connected CSRM implementation success.

In alignment with the risk-based CS framework released (CBN 2018), the CS programme must be an integral part of their risk management process and fully integrated into a financial institution's business, objectives, and goals. P8 elaborated more that:

> *The risk-based CS framework mandates clearly defined roles and responsibilities within an organisation. Implementing CS strategies and policies lies with the senior management, while the CISO oversees/coordinates the daily CS activities and mitigates CS risks. The aim is to drive CS discussions at the board level.*

P14 and P13 further comment concerning CS risk management governance structure that:

> *Today, financial organisations are hiring a CISO – Security operations no longer fall within IT. A **CISO led team** now **manages cyber risk** across financial organisations (P14).*

> *These **CSRM governance** functions are further broken down into sub-units and departments for effectiveness-managed by three lines of defence- operations/risk, control, and audit (P13)*

One immediately prominent feature is that CSRM implementation success is not a choice but mandatory.

- **Adequate Budget Planning**

Adequate budget planning is conceptualised in this study as having sufficient financial support to meet both the human capital resource needs and CSRM implementation activities and operations. Once top management members can see value and ROI in CS, it is easier to justify funding it. This has been the biggest challenge of most security leaders- communicating the value (Lee and Green 2015).

The participants unanimously agree that investment in CSRM helps implement controls to mitigate CS risk, although it is tough to attain. P11 and P14 enumerated their experiences:

> *It took **years for this communication to become effective**. Once achieved, **funding security investments** became more accessible as the organisation's exposures to more risks as the business increased its internet presence became apparent (P11).*

> *As technology leaders, we must present CS as a risk element and an investment rather than a cost centre and highlight the advantages of a matured/ proactive cyberspace. There can never be enough security investment; no company can afford a 100% security investment (P14).*

The relation between thought and action in social life can no more be conceived of in terms of wisdom than it can in terms of expertise (Geertz 1980). A CS investment that is not addressing security in any risk areas might be considered a waste. However, it will always create value if it manages risks within the business. That is why organisations consider risk appetite – the level of risk they are willing to absorb, concentrate, and invest in significant risk exposures (Fraser 2016; Purdy 2011).

One of the participants' most significant risks to the organisation is customer trust in securing the confidentiality, integrity, and availability of the large customers' data. Therefore, a massive investment in security controls against data breaches helps in fortification against CS attacks. P10 explained the impacts of adequate budget planning:

> *Adequate budget planning **creates enormous value as a success factor** for **establishing customer trust** as financial institutions are at the age of competition using **CS to outshine others** (P10).*

5.3.3.6 Evaluation of Factors for CSRM Implementation Success In Case Study B

Figure 5.15 below shows a matrix coding of the participants' overview of the factors identified.

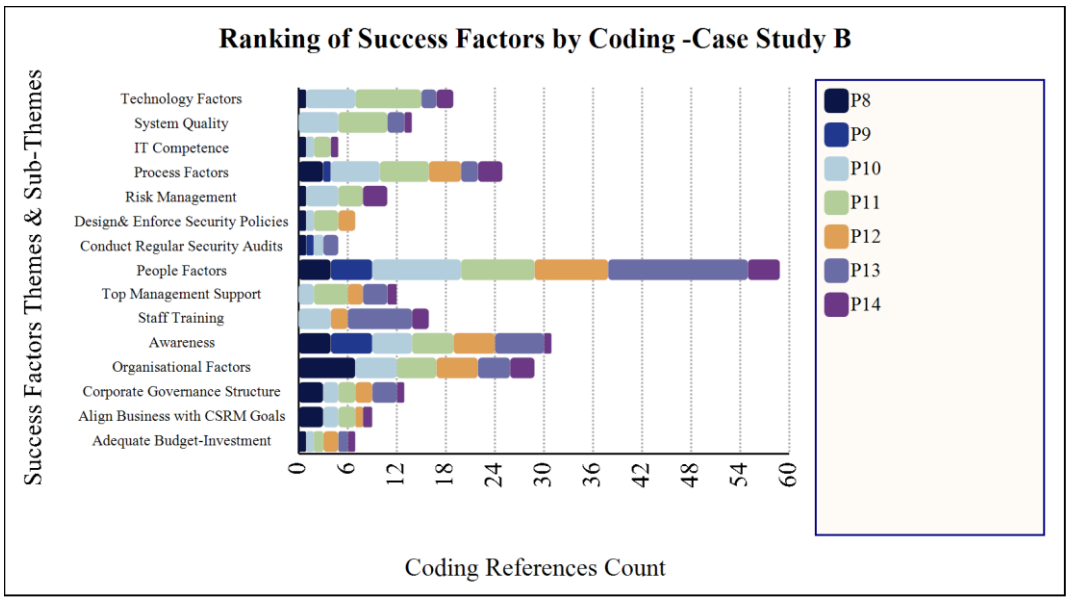

Figure 5.15: Ranking of Success Factors for CSRM in Case Study B

Figure 5.15 above shows that all the participants rank people factors as success factors higher than the other factors. At the same time, awareness and training programmes continue to be acknowledged as a success factor for CSRM implementation success. CSRM implementation success's antecedents are remarkable effects of people and organisational factors relative to the lesser impact of security controls and technology factors. Organisational factors rank second with the establishment of appropriate corporate governance, while technology factors rank lowest. Previous studies have identified people's factors (Hadlington 2017) and organisational factors play essential roles in establishing and implementing cyber/information security risk management (Tu and Yuan 2014).

Case study B thematic analysis highlights that although top management plays a significant role in creating and implementing policies and providing sufficient financial resources, quality technology is acquired. If the awareness level and the sense of involvement and support from users or people involved are low, the whole process will be unsuccessful and a waste of resources. Most of the CS risks and cybercrimes attacks exploit humans (Bendovschi 2015).

The organisation's CSRM strategy comprehensively address CS awareness and training. Thus, a constant education process, formal or informal, in CSRM awareness and training is vital for CSRM implementation success. Some participants measure the overall success of their organisations' implementation of the factors as follows:

> *In my opinion, success is a self-functioning CSRM system wherein the various stakeholders within the CSRM system- the people, process owners, and technology custodians are aware of their security roles and take ownership of security (P11).*

P10 and P12 unanimously echoed the success rate of CSRM implementation based on the organisation's performance. Measures are customer and client satisfaction, fewer incidents, and customer complaints at least the last five years.

All the participants except one indicated that all the factors had not been identified. A matric coding of the overview of the new factors shows in figure 5.16 below.

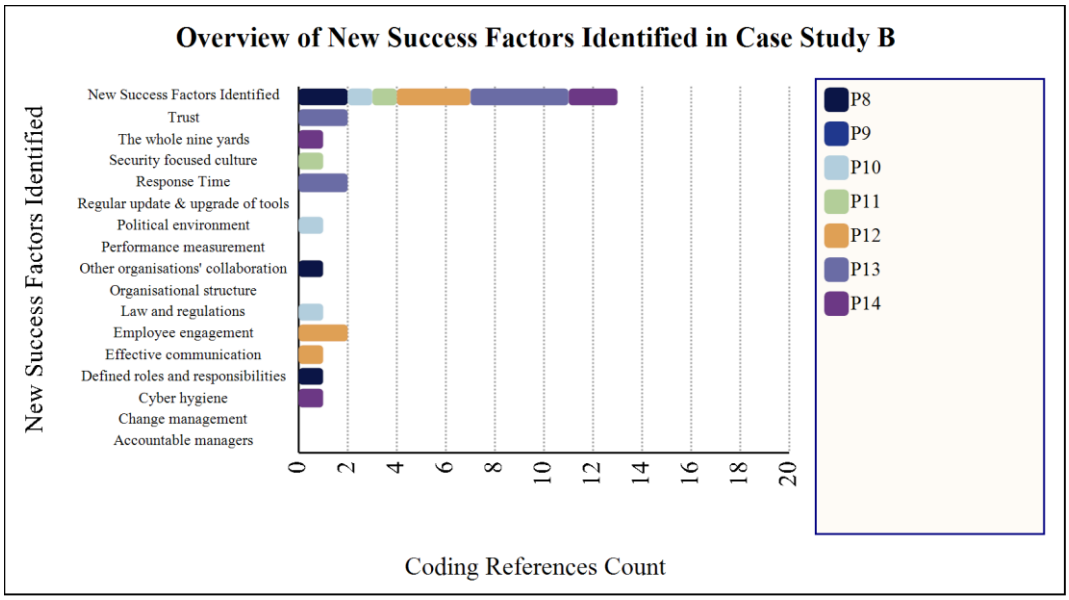

Figure 5.16: New Success Factors Identified

Figure 5.16 above depicts an overview of the factors identified by the themes and sub-themes. A review of the success factors shows other new factors that the participants believe are important to CSRM implementation success. They include:

Firstly, collaboration with other organisations in the industry. The quality, breadth, and depth of CS risk incidents of incident data reports (in most cases the impacts of the incidence) from other organisations are necessary for proper alignment of the CSRM implementation process and response (Chrapavy 2016; Zhao, Xue and Whinston 2013). However, given the importance of knowledge sharing of risk incidents data and assessments to be communicated to a higher audience, several challenges make it a challenging goal to achieve. Reputation could constitute a barrier; individuals or groups may not be motivated to report and share knowledge due to fear of unknown detrimental consequences.

Some large organisations, through cyber insurance, in a collaborative approach, share or transfer risks to achieve resilience (Sharkov 2016). Resilience management is added as a complete step to enhance CSRM through multilevel stakeholder engagements (law, governance, business initiatives) (Nicho, Khan and Rahman 2017). The transition from the CS approach to business risk management demands governance and resilience as a complete step to a practical CSRM approach (Sharkov 2016). Cyber insurance or risk transfer could be a major factor needed to organise CSRM recovery from a successful cyber incident as an optimal CSRM investment strategy (Mazzoccoli and Naldi 2020). However, arguable debates exist on cyber insurance as an approach to CSRM (Biener, Eling and Wirfs 2015; Pal 2014; Toregas 2014). All these interwoven factors agree that success in CSRM is dependent on collaborative networking of sharing knowledge, best practices and relationships (Hampton 2006).

Secondly, defining and assigning CSRM roles and responsibilities is a success factor that correlates directly with corporate governance. Important information is communicated to all stakeholders with roles and responsibilities to manage risks (Maarop et al. 2015). An interesting comment by P8 embellish this:

> *A saying goes that a goat owned by the whole village will die of hunger.*

Third, law and regulation are structures of coordination and control that accompany an organisation. Laws and regulations are legislative tools that ensure that the three integral and undeniable elements of information and CS, Confidentiality, Integrity and Availability (CIA), are managed through planning, implementation, and compliance with regulatory policies. The government agencies or regulatory authorities add these management tools with the imposition of substantial penalties for non-compliance. For example, P14 reckons Nigeria's Official National CS Policy and National CS Strategy legislative frameworks move toward CSRM in Nigeria.

Adherence to these tools, including PCI-DSS, forms the basis for organisations' good governance structure. In other words, CSRM laws and regulations guard, protect, sustain, preserve, and promote CSRM implementation success when carefully followed.

Response time is another success factor corroborated by P13 as previously identified in Case study A. Many CSRM implementation projects or projects fail due to a quick response time or time to achieve a process. Some of the participants explained earlier; it took some time to educate and highlight the benefits of CSRM to senior management to convince them to buy into formal risk management processes and CS. Also, because CS is continuously evolving and complicated, the detailed specification of CSRM implementation approaches may change over time to meet the specific needs at a certain point in time. Network problems sometimes lead to the inability to respond to urgent issues on time in Nigeria. In the words of P13:

> *The response time to respond to security issues and processes is critical in CSRM in our organisation. The infrastructure is there, but the response time is limited to human power availability.*

In agreement with the literature, time is a critical factor for project success widely identified (Project Management Institute 2009; Yaraghi and Langhe 2011). Finally, P13 identified user cooperation as a success factor for CSRM implementation success.

> *I think users' factors is a critical success factor because no matter how strong the policies are and how good the technology state is, disobedient and none supportive users will form a weak link that could turn the whole process into a mess.*

5.3.3.7 Summary of Case Study B

This interpretive research focuses on explaining the organisation's actions, events, customs, and experiences of the experts on the job as they translate to success factors for CSRM implementation success. Ranging from a self-functioning CSRM system wherein the multiple stakeholders within the CSRM system- the people, process owners and technology custodians are aware of their security roles and take ownership of CS to customer satisfaction and service availability at every point in time. Case study B participants have various perspectives on CSRM implementation success.

Case study B thematic analysis shows that top management provided support by ensuring that resources were available to identify, assess and mitigate CSRM implementation success needs. In collaboration with a good governance structure, the decision-makers were better positioned to decide and implement CSRM implementation initiatives, awareness and training programmes, technical and management solutions best suited to the bank's requirements. It is worth mentioning that case study B focused its awareness campaigns on customers and employees to achieve CSRM implementation success. Hence, roadshows as an awareness platform for customers is a remarkable one not common in the banking industry.

Assessing (information gathering of the company's security assets) an informed decision regarding an organisational CSRM is the starting point for CSRM (Ionita 2013). Enhancing a CSRM implementation success structure through awareness and training on critical CS risks and CSRM through various avenues and platforms to inform, educate and train individuals, staff, customers, and CS professionals on safety behaviours and cyber intelligence seem to be an innovative approach.

Therefore, the most striking explanation emerging from case study B is that CSRM implementation success is not a pursuit. It results from knowledge and positive attitudes towards CSRM policies and procedures, obedience to specific laws and regulations and involvement in gainful activities and programmes in conjunction with people, technology, process, and organisational factors. A comprehensive approach to CSRM, combining all these factors (organisational, people, process and technical) discussed extensively above, is necessary to achieve CSRM implementation success.

5.3.4 Introduction to Case Study C

Case study C offers banking and commercial services in Nigeria's headquarter in Lagos. It prides itself on continuously securing the personal data and the confidentiality of the numerous customers' information across more than ten countries in Africa and Europe. Develop and implement security enhancements to ensure the integrity of all their e-banking platforms.

The organisational selection reveals learning aspects; a leader revolutionising the banking industry with more than 25 years of operational experience and success in implementing CSRM for its diverse e-business and e-commerce services and solutions, above 30-billion-naira revenue

and over 10,000 employees. Based on some performance indicators, the information system auditor stated:

> *On a scale of 10, our organisation's measure of CSRM implementation success is 8. There is always room for improvement (P19).*

Some interviewees who played significant roles in implementing CSRM at different organisational levels helped obtain multiple perceptions about the success factors for CRSM implementation, presented in Table 5.8 below.

Table 5.8: Case Study C Participant's Profile

Participant	Role	Years of Experience
P15	Governance and Compliance	5
P16	Human Resource Officer	9
P17	Legal Officer	11
P18	Information Systems Auditor	1
P19	Information Systems Auditor	11
P20	End-User Support	6
P21	Chief Information Security Officer	20
P22	Risk Officer	3

Table 5.8 shows that the junior and senior participants across related departments were engaged to gain insights, verify, and compare the different viewpoints and yield better knowledge of success factors for CSRM implementation. The themes identified by the semi-structured interview questions and the coding of the interviewee's responses as emerging sub-themes show NVivo outputs in section 5.3.4.1.

5.3.4.1 Success Factors for CSRM Implementation in Case Study C

Table 5.9 shows the success factors themes and sub-themes coded as parent and child nodes in NVivo outputs.

Table 5.9: CSRM Implementation Success Factors Themes and Sub-Themes in Case Study C

Themes (Parent Node)	Sub-Themes (Child Node)
People factors	• Top management support • Awareness • Training
Technology factors	• IT Competence • System quality (Task-Technology fit)
Process factors	• Risk management • Enforce CSRM policies • Security audit
Organisational factors	• Business alignment with CSRM goals • Corporate governance • Adequate budget planning

A detailed discussion and analysis of each theme and sub-theme are below:

5.3.4.2 People Factors

Consistent with the definition of the People factors theme in this study (section 2.7.2), people factors are very critical in CS implementation success (Stewart and Jürjens 2017). The thematic analysis revealed rich information that people factors are crucial for CSRM implementation success by all the Case study C participants. The NVivo representation is shown below:

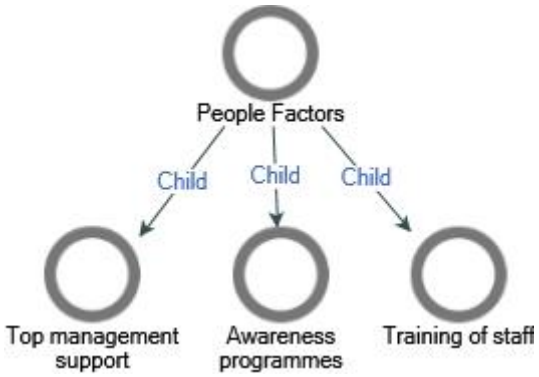

Figure 5.17: People Factors Theme and Sub Theme

The theme (people factor) and sub-themes – top management support, awareness, and training, as shown in figure 5.17 above, were used as success factors for CSRM implementation. Examples of comments from the participants supporting the identified people factors theme are discussed next.

- **Top Management Support**

Top management support is critical in CSRM implementation as, without this, there will be no investment in resources (human and financial) and approved security policies to drive the implementation. P18 and P22 explained that:

> *Without top management support, it will be challenging to implement a CSRM. Top management provides direction, resources, and commitment to the success of the CSRM (P18).*

> *Top management support is required to ensure the longevity and success of the CSRM implementation programme. For example, the end user's PCI DSS standard will be supported if the Managing Director has issued a charter stating its intentions and re-affirming his support (P22).*

The thematic analysis findings show that end-users commit to best practices if the management actively communicates the support for CSRM implementation success. These findings corroborate (Chatterjee 2019) that top management support and commitments are essential for CSRM implementation success. The information systems auditor summarised the importance of top management support:

> *Top management support is required because they drive the implementation through approved and published information/CS policies. Investments in CSRM implementation occurs where top management is in support.*

- **Awareness**

Awareness plays a significant role in this study context in supporting stakeholders towards successful CSRM implementation. Sections 2.6.2 previously discussed the various roles the awareness of top management, middle management and end-users play in CSRM implementation. The thematic analysis confirms that the participants perceived that implementing several awareness programmes via online and face-to-face platforms has benefited CSRM implementation success in strengthening transactions security. Examples include monthly intranet awareness publications, documented policies communicated to all stakeholders and sensitisations. Such include increased knowledge of cyber threats reported phishing emails and taken down of

phishing sites. Top management participation in awareness programmes helps generate staff's buy-in and commitment. In case study C, one unique awareness training is the annual cyber awareness week programme where officers win gifts for correctly answering questions. Sample comments from the interviewees, which further provide evidence supporting the awareness success factor, are:

> *The bank is continually improving its security culture through awareness programmes to drive the embeddedness of security into daily transactions (P21).*

If users fall victim to CS risk and threats due to lack of awareness, these could lead to several unauthorised activities. According to P20;

> *Awareness is driven through top-down approaches on all mediums. There is frequent engagement around CS in the organisation, and security is taken seriously; CSRM deficiency has reduced significantly.*

Training programmes have strengthened transaction security and reduced security issues and incidences in the last five years. This finding agrees with Frank and Odunayo (2013) that organisations will lose CSRM battles if security professionals are miles behind the cybercriminals.
P18's comment expressively supports this:

> *The CSRM awareness program has aided transaction security. Users are better aware of the risks associated with the activities and ensure these risks are mitigated by adhering to the recommended controls.*

- **Training**

Training programs help the employees acquire the necessary skills and knowledge to advance CS thoughts and actions to protect the organisation from any detrimental CSRM implementation failures (Caldwell 2016; Disparte and Furlow 2017). Cyber security risk management could become successful when human vulnerability to cyber-attacks could not be exploited (Bendovschi 2015). People constitute a central part of all CSRM implementation support systems (Stewart and Jürjens 2017). The literature explains effective training mediums to support people, such as face-face classroom training, blended online training modules, self–study online training and

interactive, hands-on activity-packed user involved education programmes or risk workshops (Caldwell 2016; Puhakainen and Siponen 2010).

The interview data findings from case study C provided evidence supporting CS training as a critical factor in CSRM implementation success. Most of the participants considered a combination of programmes such as Nuggets, email, on-boarding classroom training, online training courses, information security group portal, intranet publications and some specialised pieces of training, among others evidenced CSRM training importance by their comments:

> *Top management communicates its support for CSRM implementation success by approving budgets for* ***some core officers*** *to be* ***trained and certified in ISO 27001 information security implementation systems*** *(P19).*

> *The risk to the business has been reduced through awareness training. The policies and procedures state management direction for the business, and users are, therefore, contractually obligated to follow them (P22).*

However, there is a significant difference between the training staff and changing behaviour. Evaluation of CSRM training or follow up is necessary to ensure that the training is helpful for CSRM implementation success. P22 illuminates more about ensuring the effectiveness of training that:

> *Human resources sometimes test knowledge* ***to ascertain training effectiveness, and*** *any end-user deficient in knowledge will attend more training. T****hree months after any classroom training programme, supervisors evaluate the training's impact through a survey.***

Findings from the thematic analysis of the result show that frequent CSRM training and awareness on CS implementation impact the success of CSRM to no small extent in alignment with previous literature (Puhakainen and Siponen 2010). This finding articulately summarised the values of CSRM training in the words of the human resources manager:

> *Completing the bespoke e-learning courses is a criterion for employee job confirmation after the 6-months probation period. The CS week is dedicated to*

sensitising employees on CS issues and pops up tips on the intranet, reducing incidences and financial losses.

5.3.4.3 Technology Factors

The technology factors in this study are conceptualised in section 2.7.3. IT competence and system quality play a vital role in CSRM implementation success. The findings from the interview data provided evidence supporting technological factors as success factors for CSRM implementation. The participants mostly found the influence of system quality necessary in securing the various organisational vulnerabilities and endpoints, access, and transactional authentications. Most participants believed that the management had invested much in technological solutions. However, technical solutions, as well as human IT capability development, cannot be 100%. Comments expressed are discussed below:

- **IT Competence**

IT competence's conceptualisation remains unchanged (see section 2.7.3). In line with previous studies from the resource-based view, IT competence is a resource that includes capabilities, processes, attributes, knowledge, and know-how that supports the formulation and implementation of competitive CSRM strategy and business performance (Kotulic 2001; Rivard, Raymond and Verreault 2006). The importance of adequately equipped employees with the appropriate skills set for managerial or departmental positions in CSRM implementation cannot be overemphasised.

The data analysis shows that IT competencies play an important role in the IT strategy formulation by enabling proper IT support to influence successful CSRM implementation. This ensures that individuals with a good understanding of the requirements of CSRM are in place to help ensure its success. Also, IT competence helps protect customers' information and develop a mechanism to monitor their compliance with the processes using tools and regular evaluation of the processes to detect and log unauthorised system configuration.
P21 noted that:

No security breach can happen without involving end-users of IT systems.

Thus, competent IT managers enforce controls through central–managed technology. The number of vulnerable end-users shows their level of compliance with the established CSRM operational rules. Periodical conduct of awareness test and unannounced data security sweep coupled with a weekly measure of systems without up-to-date patches and antivirus measures the staff IT capabilities. Half of the participants believe that the staff's IT capability is directly related to extensive CS awareness and training that has helped accomplish CSRM implementation success. For example, P18 emphasised that:

> *More importantly, the **IT team's expertise**, a **good understanding of the requirements for CSRM** and **commitment** have been **complementary to influence** and **ensure IT support for CSRM strategy formulation** and **IT assets** for **CSRM implementation success**.*

This notion aligns with the findings from (Bassellier, Reich and Benbasat 2001; Tu and Yuan 2014) that IT competence that incorporates tacit, implicit and explicit knowledge is an essential success factor in effective CSRM implementation. IT competencies, including technical IT resources, top-down processes, and operations, strengthen CSRM implementation success.

- **System Quality**

The availability and reliability of the technology used for performing CSRM tasks play a vital role in CSRM implementation success. Findings from the participants reveal that technological solutions' availability and reliability have had a tremendous impact in protecting numerous organisational vulnerabilities and enforcing the controls put in place even when end users do not. P20 comments:

> *Technology solutions have had a significant positive impact on CSRM implementation success.*

Although technological advancements continue to increase with the rise in cybercriminal activities, a suitable set of technical solutions has been deployed to achieve a certain optimal level of CSRM. Among the available and reliable technological solutions used for CSRM implementation, according to their comments, are: SIEM for log management, Vulnerability Assessment tool and a network monitoring tool to managed availability of devices, use of passwords, biometric and onetime passwords, Multi/2FA factor authentication for remote support

of access and transactional authentications, Web application firewalls and Advance Persistent Threats tools. P22 attested that:

There can never be 100% security, but we are confident that we can mitigate about 95% of the identified threats through the vulnerability assessment software.

This agrees with other information systems socio-technical studies that the technology used for CSRM tasks covers all aspects of risk management and improves the use of technology for risk management (Lyytinen and Newman 2008). Further emphasises the importance of recognising system quality's centrality – the availability of well-proven and reliable technology used for CSRM implementation (Lyytinen, Mathiassen and Ropponen 1996).

5.3.4.4 Process Factors

The process factors are the processes of risk management and controls for CSRM implementation success. The process factors represent various risk management tasks of identifying CS risks, executing quantitative analysis and qualitative analysis, formulating and communicating risk responses, monitoring and controlling CS risks that help manage CS implementation in organisations. The identified sub-themes include Risk management, CSRM policies and Security Audit.

- **Risk Management**

There are broad perspectives and various international agreements on the growing importance of risk management in CS/information security (section 2.5.1). This accounts for an increasing range of frameworks, capable methodologies, tools, techniques and vast practical implementation of CSRM across many organisations.

The participants agree that the risk management process/procedures ensure CSRM implementation success. Likewise, the organisation employs a combination of risk management approaches as the best way to effectively manage CS risks by identifying and implementing a set of standards and appropriate controls. The interviewees' responses substantiate the findings of the interview data:

We have implemented international and local standards to ensure the success of CSRM (P21).

These standards include the combination of ISO 27001, PCI-DSS and CBN CS framework to identify, analyse, evaluate, treat, and monitor risks (P19).

Inexplicably, the participants did not elaborate much on each phase of the risk management process, but P18 affirms that:

*The **key risk management components** of the **standards/frameworks** have been **very effective in identifying and reducing cyber threats and attacks in the organisation.** **T**hey are reviewed regularly for relevance.*

A further probe into how CSRM is achieved in the annual report revealed that an IT risk management committee is responsible for ensuring continuous IT risk management expertise development. The committee establishes standard IT risk management practices and ensures compliance for institutionalising IT risk management in the Bank's operations at all levels; and identifying and implementing cost-effective solutions for IT risk mitigation (Annual report 2018: 26).

This concurred with the previous study's findings that found CS frameworks fragmented and vary in effectiveness (Atoum, Otoom and Abu Ali 2014). Hence, following and breaking down the internationally agreed and tested risk management standards/frameworks into tasks and sub-tasks (identification, analysis, and response planning) for enhanced CSRM implementation may reduce complexity and achieve objectives.

- **CSRM Policies**

The enforcement of security measures, countermeasures, and protective procedures in security policies is essential as part of organisations' living documents. When integrated into business processes in achieving successful CSRM implementation and broader organisational objectives, cyber security risk management policies and procedures help focus more attention on the identified CS risks and threats from risk analysis (Spears and Barki 2010). The analysis of the participants' comments and findings confirm CSRM policies as a success factor for CSRM implementation success in case study C. For instance, P18 and P21 stated:

The bank has placed multi-layered defences and devotes attention to the most critical risk factor - the 'human firewall' through policies. ***Security policies*** *have effectively reduced CS breaches in the last five years (P21).*

CSRM policies *have* ***been relatively helpful,*** *but as technology advances, the sophistication of attacks advances. H****owever, these policies remain effective****—no CS breaches in the last five years (18).*

The numerous security policies include password policy (alphanumeric passwords and frequent password change), network management policy, management of technical vulnerabilities, access control policy (Two-factor authentication for login) and acceptable use policy.

Many analyses of the findings align with a positive and significant relationship between critical elements of cyber security/ information security policies management and the organisational cyber/information security effectiveness programmes in Nigeria and other developing countries from previous studies (Al-Awadi and Renaud 2007; Okolo 2016). Recognising the relationship between the user-friendliness/compliance and effectiveness of CSRM policies (Dawson 2018), employee engagement through adequate awareness and training remains the effective way of guiding stakeholders' actions and emphasising CS policies (Siponen, Mahmood and Pahnila 2014).

- **Security Audit**

One might be prompted to ask – What is the point of having CS policies if they cannot be regularly enforced, monitored, and measured for compliance? Security audit evaluates, monitors, measures and report compliance with security policies, guidelines and controls (Singh, Gupta and Ojha 2014). It is important to note that the security audit's resultant effects lead to monitoring and assessing compliance and lead to the identification and discussion that promote collaboration and integration of security controls and corporate governance for effective management decisions.

The participants unanimously agree that a security audit has been a critical success factor for CSRM implementation. Explaining more on the importance of security audit, the participants' comments:

*The **security audit has been very effective**, covering the technology and end-to-end processes (P22).*

A security audit's overall benefits ensure that the controls and policies are efficient and sufficient to meet CSRM implementation success requirements (P18).

The participants' comments substantiate literature that security audit highlights how well the security implementation processes are performing and areas that need improvement (Islam, Farah and Stafford 2018). Security audit provides insights into the road to CSRM implementation success. However, the woods are still eager for interpreters (Geertz 2004) (managers/board) to grasp and combine the organisational factors with the previously discussed factors to ensure businesses and organisations do not suffer enormous CSRM implementation challenges and consequences.

5.3.4.5 Organisational Factors

The organisational factors align the CSRM strategy, processes and practices with the overarching corporate strategy and specific business needs (Hudin and Hamid 2014; Shah, Jones and Choudrie 2019). Organisational factors represent essential factors that influence CSRM implementation success. The sub-themes that emerged are Business alignment with CSRM goals, Adequate budget, and corporate governance.

- **Business Alignment with CSRM Goals**

In this study, the alignment of business activities and goals with CSRM goals ensures that risk management processes/tasks and goals fit well with other CS activities, business values and organisation needs. The emerging business-driven organisation supports a paradigm shift from technical solutions to value-driven practices (White et al. 2020). Organisational factors highlight aligning CSRM implementation strategy to business strategy with the organisational objectives (Spears and Barki 2010; Tu et al. 2018). Business alignment enables enterprise-wide support at all levels, sound practices and the provision and deployment of essential resources for CSRM implementation success (Atoum, Otoom and Abu Ali 2014).

The participants acknowledge that business alignment with CSRM goals is an important success factor in CSRM implementation success with different interpretations. P19 articulates these views:

> *The recognition by management and regulators that the use of information technology to drive business also introduces CS risks which is now an inherent risk in business, causing* ***CSRM function to align with the rest of the business****.*

The alignment ranges from the design and the infusion of CSRM based on several frameworks into the bank's policies and controls to mirror its goals. That is, the policies closely align with the business objectives. For instance, a broad understanding of the CSRM controls helps build industrial capacity and ensure customer data integrity, affecting its reputation. P20 beautifully summarises this alignment:

> *The information security committee responsible for the CS programme's governance* ***designed it such that CS, risk management framework and strategy align with the rest of the business*** *by* ***taking them into account when making critical business decisions*** *and* ***setting business objectives.***

The comment suggests the direct relationship of the findings with previous literature (Srivastava 2017). Understanding the business structure-strategy alignment forms the bedrock for the successful execution of CSRM implementation and organisational performance.

- **Corporate Governance**

For CSRM to be effective in an organisation, management and the board must dictate the tone for the governance of CS accountabilities and responsibilities of managing security risks to digital information assets. Corporate level management of security risks is imminent since IT aligns all business processes and resources for optimum security performance of protecting digital and non-digital information assets from internet-related risks and competitive advantage (Turel, Liu and Bart 2017).

Directing and controlling the CSRM function through corporate governance form an integral part of management's strategic competencies (Chatterjee 2019; von Solms and von Solms 2018). Thus, corporate governance spans all business functions as most business activities depend on the internet; hence, the greater exposure to the CS risks and threats (Allen et al. 2018; van Erp 2017).

The interview data findings in Case study C are consistent with the above literature supporting corporate governance as a success factor for CSRM through an element of control that clarifies

essential roles and duties. The evidence expressed by the governance and compliance manager comments:

> *We are more inclined to the more **organisational approach** than a technical approach to **corporate governance** by establishing a **dedicated Board Committee with oversight functions** to **improve CSRM.***

Most of the participants stress the effectiveness of the dedicated CS team. They mentioned that C-suite executives are the key decision-makers. Simultaneously, the information security experts and compliance teams now take a seat at the table as part of conversation and decisions regarding CSRM knowing fully well the financial and reputational costs of when things go wrong due to security incidents attacks. The information security auditors (P18 and P19) advance this point:

> *Suitable IT governance structures have been put in place to measure the CSRM success or otherwise from time to time through continuous evaluation and feedback established through proper and effective governance (P18).*

> *Corporate governance has provided the direction for CSRM implementation. The CS posture is assessed through regular reporting to the information security steering committee and improving learning points (P19).*

- **Adequate Budget**

Adequate budget planning is crucial to support and perform CSRM processes. It cannot be ignored to ensure that financial resources are strategically conceived and invested to cover all the optimal investment levels for necessary costs to perform CSRM operational activities and their needs (Bojanc and Jerman-Blažic 2008; Ekelund and Iskoujina 2019). These costs include purchasing new assets for data protection and existing assets maintenance, human capital (in-house staff and experts, training) and the cost to succeed in CSRM measures and processes (Al-Awadi and Renaud 2007; Disparte and Furlow 2017). When the investment exceeds the perceived benefits, such CSRM costs cannot be considered successful (Srinidhi, Yan and Tayi 2015).
Analyses of participants' responses supported the fact that the success of CSRM is dependent on the level of investment allocated to CSRM. The CISO analysed thus:

> *CSRM Investment is directly proportional to the value created across the enterprise.*

The words of the human resource manager brilliantly summarised the effect of adequate investment in CSRM:

> *Adequate investment in CSRM over time is Impactful. High-end and top-notch CS solutions have reduced the number of CS incidents and e-fraud. For example, implementing dual authentication for some employees after one of the bank's fraud helped reduce subsequent episodes. The resultant value derived is the reduction in loss of funds, more substantial brand equity, enhances investor confidence and deepens customer trust in the bank.*

5.3.4.6 Evaluation of Factors for CSRM Implementation Success in Case Study C

Analysis of the success factors review overview shows that five out of eight participants agree that all the factors are success factors for CSRM implementation success. In contrast, others could only comment on their specific roles. However, 50% of participants believe that some factors are critical to CSRM implementation success. A matrix coding of the overview of the factors shows in figure 5.18 below.

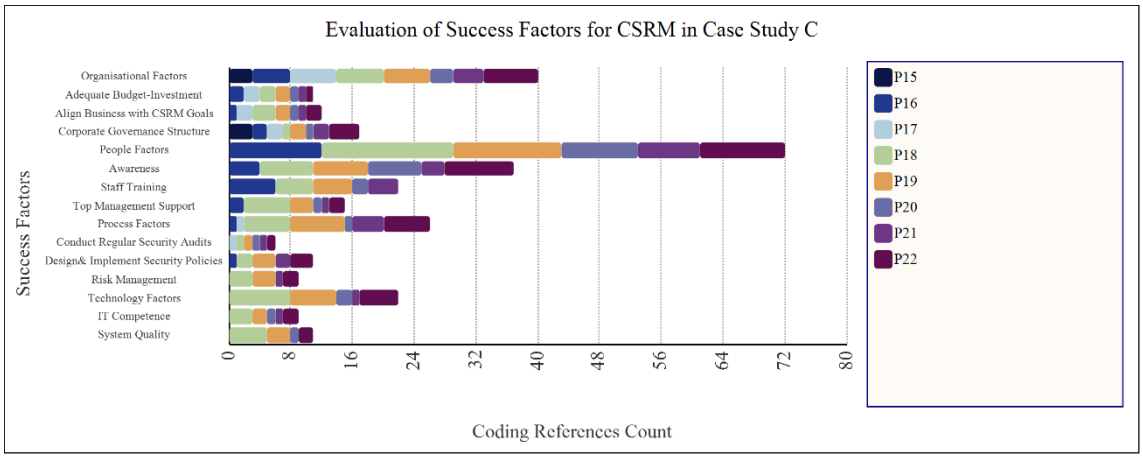

Figure 5.18: Evaluation of Success Factors for CSRM in Case Study C

Figure 5.18 above shows that although the participants' identified all the factors as success factors for CSRM, mixed feelings of some factors are more critical than the others. This more solid, empirically based investigation into success factors also enables the participants to freely express their views of the overall success factors for CSRM implementation discussed. Some of the

participants chose to rank the success factors in order of importance. The ranking was applied based on figure 5.18 above. The following risk factors ranked highest: seventy-five per cent of the participants ranked people factors as success factor first, followed by organisational factors, process factor ranked third, while technology factors ranked lowest. Awareness and training ranked first as a success factor for CSRM implementation success among people factors followed by top management support. This difference is because people's risk/ human factor is a significant factor that causes CSRM implementation success/failure. This assertion agrees with most literature that employees' adequate training, awareness, and commitment to best practices are critical to CSRM implementation success (Hadlington 2017). The effectiveness of awareness and training in the organisation is represented in figure 5.19.

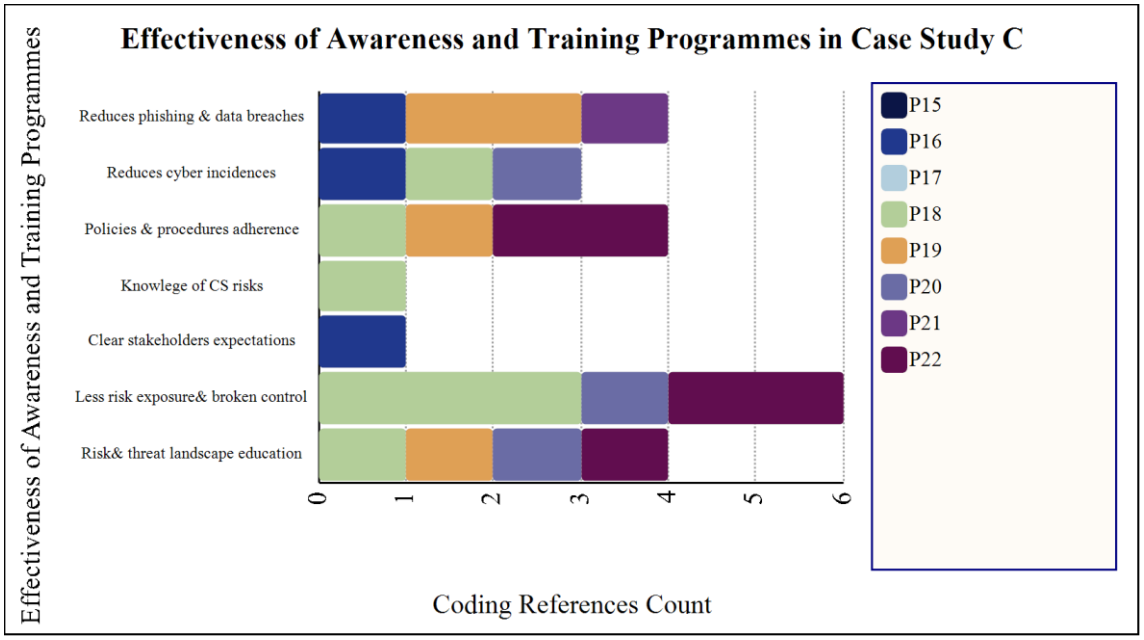

Figure 5.19: Effectiveness of Awareness and Training in Case Study C

According to figure 5.19, awareness and training educate staff, users, stakeholders on attacks and CS risks and threat landscape, ensuring strict adherence to policies and procedures. Armed with the knowledge increases the uncertainties regarding expectations, roles, and responsibilities. Reduction in the number of broken controls and risk exposures increases the capacity to reduce phishing and data breaches and reduce financial losses, at least none in the last five years. All these value-laden benefits constitute some of the measures of success identified by the participants. In agreement with the words of P19 and P20;

Top management support increases the efficiency of CSRM (P19).

Human factors are critical. Top management commitment and support are essential, investment is necessary, and the appropriate technology solution is vital in protecting organisation vulnerabilities (P20).

Corporate Governance has provided the direction to implement CSRM with various governance structures responsible for driving the adopted risk management standards and compliance with the organisation's processes, policies, and procedures. The organisation seems much more inclined to organisational factors for effective CSRM than technical and process factors. There is much more direct alignment between the people factors and organisational factors. Organisational factors rank second by establishing an appropriate corporate governance structure, as strongly expressed in the participants' interviews.

The responses showed that the system's quality adopted in the organisation also plays an essential role in CSRM implementation success. P18 noted:

Although individuals with a good understanding of the requirements of CSRM are in place to ensure its success, technology solutions have had a tremendous impact in protecting numerous vulnerable assets as they enforce the controls even when users do not.

The efficiency of security audits rated 90% by most responses as monitoring of CSRM implementation process ensures the controls are efficient and effective to achieve CSRM success. A security audit reveals how well the organisation is performing and identifies crucial areas of improvement.

A measure of the overall success of CSRM based on these factors expressed by the participants encapsulate the perceived values derived from each of the factors and several metrics defined by the CBN's CSRM framework and ISO 27001. More importantly, the successful integration and implementation of CS tools and applications led to reduced erring employees. The resultant increase in the customer base and willingness of customers, primarily corporate customers, to work with the organisation after reviewing the CSRM serves as a unique selling point.
A matric coding of the overview of the identified new factors is shown in figure 5.20 below.

5.3.4.7 New Factors Identified

Three new factors identified are the rate of change management, employee engagement and trust, as shown in figure 5.20.

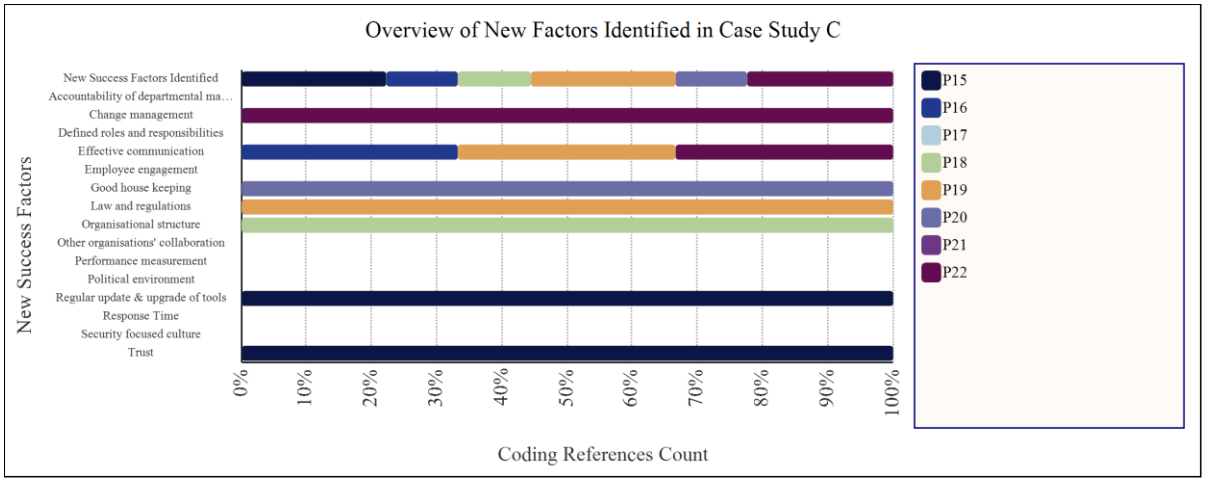

Figure 5.20: Overview of New Factors Identified

According to figure 5.20 above, the change rate is rapid to meet its agile environment due to the ever-dynamic security threats. Regulatory requirements for implementation and continuous monitoring are necessary to keep abreast of the CS domain. The rate of change management comprising effective communication channels to stakeholders and what needs to be achieved, the process, techniques, and tools to manage people, and the required business outcome must be dynamic. One of the participants explained that there is less time for threat modelling. Hence there is the need for immediate response to risk events. Employee engagement and commitment to best practices through adequate investment in human capital will enhance a cyber free organisation to a great extent if not eliminated. All the staff positively commented on the massive investment in human capital, which has helped build trust with new and existing clients. This approach has become a unique selling point, especially with corporate clients.

Figure 5.21 depicts the measures for evaluating the overall success factors in case study C, summarised in the next section.

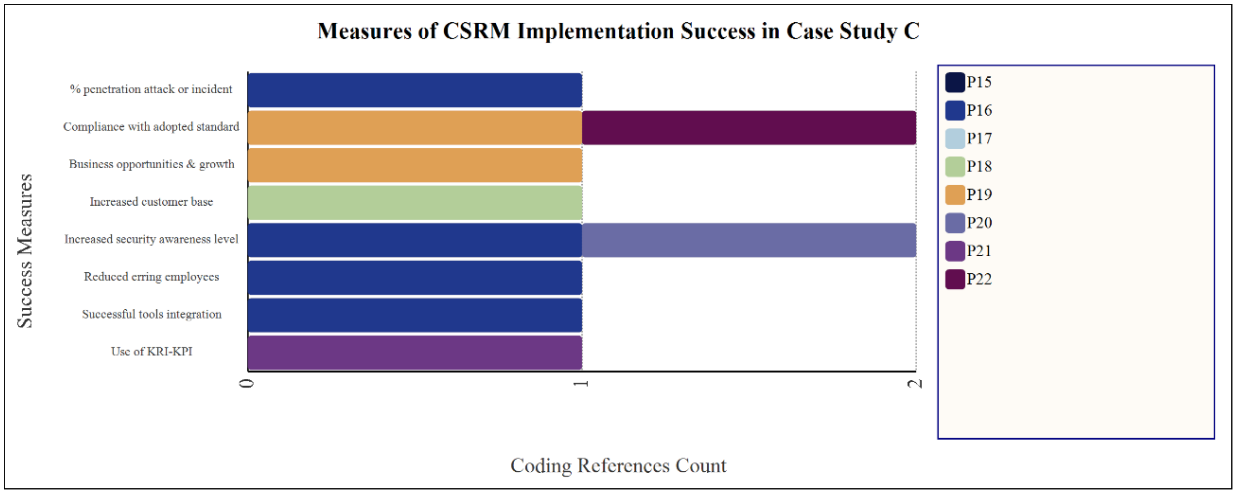

Figure 5.21: Evaluation of Overall Success Factors for CSRM Implementation in Case Study C

5.3.4.8 Summary of Case Study C

The thematic analyses of case study C concluded that CSRM implementation was successful based on the proven effectiveness of the identified factors. Governance by the CSRM steering committee, the adopted principles of the holistic risk-based approach, the effective communication channels of awareness and training on CS risks and threat landscape, tools and applications, monitoring compliance with policies and feedback on appropriate controls constitute the bedrock of CSRM success in cases study C. The critical support and commitment of the management of case study C towards CSRM based on the participants' explanations are evident.

The fact that the executives participate in user awareness training goes a long way to cooperate with staff's generality. Training and certification of crucial CS officers on ISO standards attest to key staff's IT competence and capabilities (treated like the kings) in CSRM implementation success requirements. KPI/KRI, such as increased workforce awareness of CS risks and issues, percentage of the penetration of cyber-attacks and incidents, a significant reduction in erring employees, improved business opportunities, and increased customer base and customer satisfaction, signify maturity level of CSRM in case study C.

The data analyses of case study C offer compelling evidence that the identified themes (People, process, technology and organisational) and sub-themes are success factors for CSRM. Although most interviewees rated their CSRM excellent as overwhelmingly testified by few customers, the CISO and the information security auditor with over 20 and 11 years of experience respectively

commented that there is still room for improvement. Improving security culture drives the embeddedness of matured security programmes into daily transactions. It puts multi-layered defences and attention to the most critical risk factor - the 'human firewall'.

5.3.5 Introduction to Case Study D

Case Study D is a supervisory and regulatory bank in Nigeria. As part of a core supervisory functions of the Bank, effective Ist January 2019, the Bank enforced compliance that Deposit Money Banks (DMBs) and Payment Service Providers (PSPs) incorporate risk-based CS Framework and Guidelines with their enterprise risk management framework and governance requirements as a baseline for implementing CS programmes towards enhancing their safety, soundness of functions and operating environment and resilience. The framework's essential components are CS Governance and Oversight, CS Operational Resilience, CSRM System, Metrics, Compliance with Statutory and Regulatory Requirements and Monitoring and Reporting (CBN 2018).

The CSRM system comprises four major activities: Risk assessment, measurement, mitigation/treatment and monitoring and reporting. Thus, the selection criteria for this purpose were: its success in ensuring and enforcing the CSRM framework and guidelines to assist financial institutions in achieving CSRM implementation success. The organisation has been in operations for over a decade with its strategic leadership and beneficial decision making with more than 10,000 employees. P25 thinks that:

> *The bank has achieved a more than 70% success rate. The issue of crashing into bank servers to steal information has drastically reduced in the last six months.*

5.3.5.1 Success Factors for CSRM Implementation in Case Study D

The thematic analysis contributed rich information about the success factors that can influence CSRM implementation in an organisation in this section. Based on the transcripts of the semi-structured interview protocol responses, the interviewees shared their experiences to answer the main research question to identify those factors that impact CSRM success in large organisations in Nigeria. The coded themes represent the identified factors, and the sub-themes emerge from the participant's responses, as shown in Table 5.10 below.

Table 5.10: Success Factors for CSRM Implementation in NVivo Software

Themes (Parent Node)	Sub-Themes (Child Node)
People factors	• Top management support • Awareness • Training
Technology factors	• It competence • System quality (task-technology fit)
Process factors	• Risk management • Enforce csrm policies • Security audit
Organisational factors	• Business alignment with csrm goals • Corporate governance • Adequate budget planning

5.3.5.2 People Factors

The people factors theme is consistent throughout this study (see section 5.3.2.2). Case study D analysis attests to all interviewees' importance of people factors in CSRM implementation success. Effective human resource practices at different implementation processes enhance the CSRM success rate. The identified sub-themes, top management support, awareness and training of employees show as NVivo output in Fig 5.22 below:

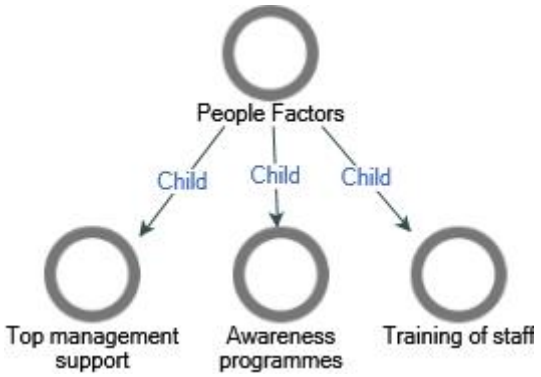

Figure 5.22: People Factors Sub-Themes for Successful CSRM Implementation

- **Top Management Support**

Top management support and commitment are critical success factors for CSRM and must be a continuous process throughout the CSRM implementation lifecycle from the respondents'

perspectives. This affirmation is scarcely different from the previous case studies. However, the participants explained that top management must be well informed of why CSRM matters, not technical jargon, to get their expected commitment and support. Evidenced by P23 and P26:

> *Top management support is compulsory; it is not an option. Management does not want technicality but straightforward explanations devoid of technical jargon! Sir, you will lose hundreds of billions; these are the risks; our organisation will lose an average amount of reputation. Top management would like to hear all these because they sign the cheques (P26).*

> *We have **management buy-in supporting us** in our CS programme. Although it took a long time to realise that CS **is key** to the business, now they are giving the **needed attention** (P23).*

Therefore, Top management receives a monthly report of all issues in all banks. As a regulator, determines the kind of CS training and workshops to support DMBs and PSPs.

- **Awareness**

The interviewees share many similarities with prior findings from case studies and literature that awareness plays a vital role in CSRM implementation success. P24 and P25 comments:

> *Generally, I think that awareness is very high compared with five years ago. It would be tremendous to increase awareness continuously (P24).*

> *Awareness does a lot! It does a lot, especially two major security issues (phishing and social engineering) within the security breaches we have across the world (P25).*

There is strong evidence suggesting the undoubted level of importance attached to awareness initiatives/programmes in case study D. Most organisations' awareness mediums/initiatives are screen savers, digital training programmes, onboarding training and emails. Among the measures of understanding and overcoming employees' vulnerabilities is testing their current level of awareness and vulnerabilities by competent awareness training officers (Hussain and Skinner 2019). Remarkably, case study D goes a step further at the organisation's operative arm by

organising dedicated awareness training sessions, particularly those who failed awareness evaluation tests multiple times after training. Unusual though, P26 explained that:

> *An aware staff poses less risk to the organisation, so if a staff fails numerous times, others call in to have an honest discussion about putting them through.*

Also, the bank conducts a combined, targeted quarterly awareness education for top management and board members.

- **Training**

Case study D performs a dual role as a regulator and supervisor. At the supervisory level, it acts as an examiner and conducts IT surveillance and CS check on commercial banks and issue advisory notices to banks on threats or vulnerabilities that have been noticed. Then, conduct CS seminars on issues expected to be taken home to their institutions to increase their CS posture. Also, ensure that the CISOs have up-to-date knowledge and information on CS through attendance at international conferences.

Staffs at the operations arm undergo periodic new skill development training such as threat hunting, malware, forensics, machine learning and artificial intelligence to put more controls in their networks as new developments in the CS domain unfold globally. A table-talk training is organised for top management, governors, and directors on CS at least once every year. A network security officer comments on training as a success factor for CSRM:

> *In recent times, CSRM* ***training has been effective.*** *I have understood many things better than some years ago on the job.* ***The ability to perform well*** *is* ***more of those pieces of training*** *received.*

5.3.5.3 Technology Factors

Technology factors rank among essential factors to accomplish many organisational CSRM implementations activities. Participants identified the crucial technical factors coded as emerging sub-themes represented as IT Competence and System Quality.

- **IT Competence**

IT competence is conceptualised as the combined and interrelated capabilities of technological resources to fulfil its business and security objectives consistently. The participants acknowledge that IT competence is necessary but stressed that CS is more than an IT issue, as substantiated by previous findings (Chabinsky 2014; Chang, Chen and Chen 2011; Kayworth and Whitten 2010). Knowing that CS is not just about investment in technology, ensuring an adequate staff supply with the required CSRM implementation success skills is inevitable.
P23 pointed out that:

> *The CS strategy group from critical departments within the organisation collaborates with the **few dedicated, committed, and passionate CS skilled force**s and CS programmes; it is not for everybody.*

- **System Quality**

The choice and implementation of an appropriate technology that ensures a productive outcome between the organisation, people and the process are paramount for CSRM implementation success (Palvia, Sharma and Conrath 2001). Case study D as a supervisory institution exemplifies the importance of system quality in CSRM by looking at eight key risk areas where a close fit between technology, people, process, and organisation is paramount. These key areas are:

1. IT destruction-e.g., denial of service
2. Data loss-data warehouse for other banks and other financial services
3. Third-party risks –by interconnections with other banks as a regulator.
4. Insider risk information leakages are crucial players in financial and government institutions and the country's economy.
5. Regulatory risk (Nigerian data protection policy).
6. Reputational risk.
7. Fraud and Data theft (government and financial services institutions).
8. Human resources risk.

Based on the above risks, P23 explained that the institution leverages defence-in-depth by relying on **state-of-the-art technology,** especially **new technology** like Artificial intelligence and

machine learning for CSRM. More importantly, all-day monitoring of the network, incidence response, and any disaster recovery.

5.3.5.4 Process Factors

The process factors include the process of risk management and controls for managing CSRM implementation success. These factors include various risk management tasks for managing CS risks and implementation in organisations. The identified sub-themes include Risk management, CSRM Policies and Security audit.

- **Risk Management**

Risk management continues to apply to CS. This accounts for a growing range of frameworks, body of knowledge, capable methodologies, tools and techniques and vast experience of practical implementation of risk management and its applications in CSRM across many organisations.
Risk Management is one of the Cyber Security Capability Maturity Model (C2M2) domains the Institution has aligned and adapted for its CS maturity. Risk management aims to identify, analyse, and mitigate CS risk to the organisation, including its business units, DMBs and PSBs, connected infrastructure and stakeholders.

One participant explained that risk management helps establish a CSRM strategy and manage CS risk and management activities. The high-level CSRM program developed identifies its threats, vulnerabilities, risks, risk tolerance and strategy for implementing, monitoring CS risks, and evaluating compliance measures. The CSRM strategy includes a risk assessment methodology, risk measurement, mitigation/treatment, monitoring and reporting. Within this program, identified risks are documented in the risk register. The risk tolerances are recorded to ensure that they are monitored and responded to promptly. Other domains in the adapted C2M2 model, such as asset management, event, and incident response, change configuration management, threat and vulnerability management and situational awareness, refer to the risk register. The CSRM program connects and strengthens all the practices in the model.

The change advisory board lead is resident in the quality and compliance, and the security team evaluates and approves the implementation of new CSRM initiatives. The senior management and Board of Directors comprised some independent members. The audit risk committee reviews

the risk management reports and CSRM programme annually for informed decisions to ensure that it remains aligned with the organisation's strategic business objectives.
Thus, the data analyses from participants confirm the strict adherence to risk management best practices as a success factor for CSRM implementation in case study D.

- **CSRM Policies**

Security controls in the form of clearly communicated policies heighten awareness of security, help establish protective procedures and drives compliance with a potential to reduce vulnerabilities and CSRM implementation success significantly. CSRM policies, when integrated into business processes in achieving successful CSRM implementation and broader organisational objectives, help enforce security measures, countermeasures, and procedures. The analysis of the participants' comments and findings confirm CSRM policies as a success factor for CSRM implementation success in case study D. P24 and P25 stated:

> *Security policies give us a framework and direction (P24).*

> *The overall CSRM policy is one-there is zero tolerance to non-compliance and key relationship management (P25).*

The above statement agrees with prior studies that well-designed security policies are a prerequisite to implementing effective security management programmes (Siponen, Mahmood and Pahnila 2014; Dawson 2018).

- **Security Audit**

CS policies and conformance levels should be auditable at intervals as much as possible. Internal security audits prevent management misconduct (Ege 2015), quality financial reporting (Christ et al. 2015) and increase internal control and compliance processes (Lin et al. 2011). Analyses of the participants' comments show that security audit has been a success factor for CSRM success by giving CSRM visibility at the board.

> *The audit effectively covers the technology and the end-to-end processes (P29).*

> *The audit highlights the areas of weaknesses for remediation actions (P30).*

Nothing could be hidden from the audit risk committee, like a checkmate, even if our management wants to hide (P23).

The findings support prior studies that security audit has been a success factor for management, policymakers, boards in formulating an effective CSRM program (Ege 2015; Islam, Farah and Stafford 2018).

5.3.5.5 Organisational Factors

Organisational factors align the CSRM strategy with the overarching organisational strategy and specific business needs. Organisational factors differentiate management practices and concepts in aligning technical and non-technical aspects to achieve CSRM implementation and its strategic goals. The sub-themes that emerged are Business alignment with CSRM goals, Corporate governance and Adequate budget planning.

- **Business Alignment with CSRM Goals**

The alignment of business goals with CSRM goals means ensuring a close fit between business activities and managing cyber security risk activities in the organisation. A strategically focused or business-driven CSRM implementation strategy is vital and should align with the organisational objectives to be successful (Spears and Barki 2010; Tu et al. 2018). Business alignment gives impetus to the investment of necessary resources and acceptable CSRM implementation practices (Atoum, Otoom and Abu Ali 2014).
Participants from Case study D confirmed that business alignment with CSRM goals is a critical success factor in CSRM implementation. P26 explained how the business aligns with CSRM goals:

We hand-picked mostly all the frameworks to align with the Bank's business needs and CSRM goals. We have frameworks, guidelines, best practices that align the goal such that we can compete with developed countries and everybody in the world in terms of best practices for CSRM success.

The CS programme and strategy cover internal threat intelligence through brand monitoring and are regularly reviewed to update its vision and mission.

- **Corporate Governance**

Appropriate oversight and governance structure in an impactful, more business-security oriented fashion can effectively manage cyber security risks. Case study D is more of a role-based organisation such that the CSRM implementation function is divided into units. The mapped phases of the C2M2 model, identification, implementation, monitoring and evaluation (compliance) teams are different units. In the words of P24:

> *No staff will be able to partake in every aspect of CS;* ***if one unit does everything*** *that pertains to our security, it is also a risk. So, one division monitors, the other implements.*

As a regulatory institution, the CS Strategy Group governs CSRM. This group consists of the banking supervision team, IT departments and other key departments. The group meets regularly and review the CS programmes for the DMBs and PSPs. The bank's examination department oversees and supervises the commercial banks' CS in Nigeria. The organisation's risk management team is separate and different from the IT risk management. The CISO reports directly to the chief executive. A non-executive member heads the Board made up of the audit risk, CS committee and the executive directors. An aspect of the governance of CSRM is the command structure in which an independent CISO in all DMBs and PSPs must be established and must be at least an assistant general manager. P23 summarised thus:

> *The governance structure has helped checkmate CS risk level and assurance of CSRM success.*

These governance structures show that cyber security risks managed at the corporate level with the same attention as other financial, operational, or regulatory risks guarantee the continuous visibility of CSRM activities and reports. An appropriate governance model ensures implementation success. This analysis agrees with the literature that corporate governance is critical for managing cybersecurity risks and their implementation success (Allen et al. 2018).

- **Adequate Budget**

Top management support with adequate financial resources provides a solid foundation for a successful CSRM (Gordon, Loeb and Zhou 2016). The participant commented that sufficient

investment in CSRM is necessary for a successful CSRM. Although there is management support in investment in CS, there is room for improvement. There is the challenge of acquiring and sustaining human resources, especially in specialisation areas, forensic experts, malware experts and desired state-of-the-art technology. P23 passionately explained that:

> *Gartner, an independent research institution, recommends that IT have about one-third of the institutions' entire budget because about **25% of the IT budget** should go **to CS for investment in technology**. However, for now, our **investment** is not reaching 25%. Hence, the conclusion that we are still lagging but not doing badly.*

Contrarily, some participants at the operations arm, unlike the regulatory arm, believe that the organisation has demonstrated an excellent investment in firewalls and monitoring devices, including intelligence, monitoring and considerable investment in staff and technical staff awareness. P24 added:

> *If there had been no **investments**, I think we would be open to any attacks; they have significantly invested.*

The above comments highlight the importance of adequate budget planning as a success factor for CSRM supporting literature (Al-Awadi and Renaud 2007).

5.3.5.6 Evaluation of Factors for CSRM Implementation Success in Case Study D

Case study D evaluates the CSRM success by adapting and measuring the CS Capability Maturity Model (C2M2) from the US energy department to evaluate, prioritize and improve their CS capabilities. The model focuses on implementing and managing CS practices associated with the operation and use of information technology and operational technology assets and the environments in which they operate. Many participants believe that their CSRM has achieved above 70% success as a regulatory institution even though the roll-out of full compliance with the CSRM framework is still at the embryonic stage. According to P24 and P27, this is because:

> *We have a lot of management commitment from banks, MDs and CEOs are now much more aware of cyber risk and the importance of proper management (P27).*

The crashing issues into the bank's servers have drastically reduced in the last six months based on the number of assessments carried out within the year (P24).

Analysis of the success factors review overview shows that all the participants agree that all the factors are success factors for CSRM implementation. P27 and P28 comment:

Every organisation has people, process, and technology (P27).

These identified success factors are very germane (P28).

The overview of the matrix coding of factors represents the relationships between the themes and sub-themes, shown in figure 5.23 below.

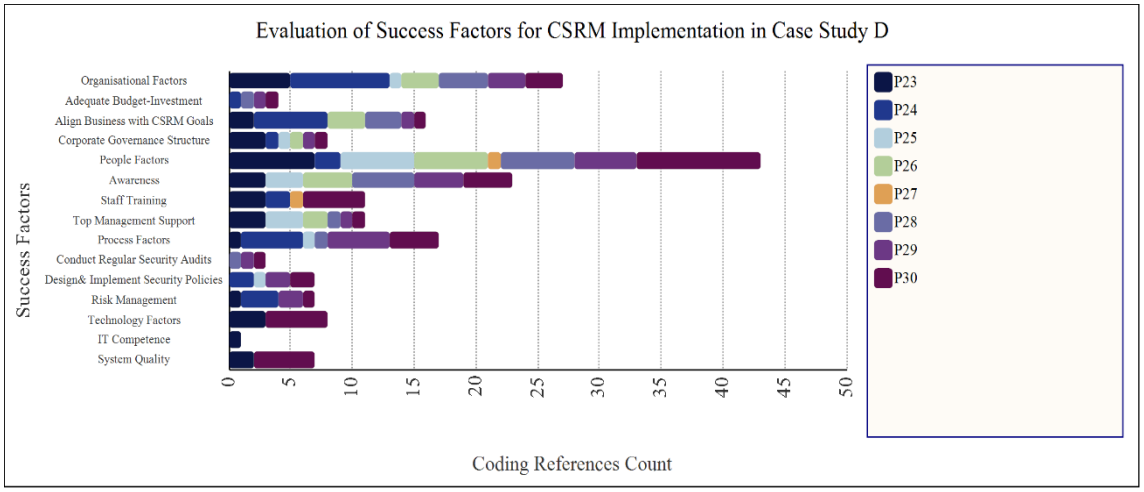

Figure 5.23: Evaluation of Success Factors for CSRM in Case Study D

Figure 5.23 above shows people factors as success factors first, followed by organisational factors, process factors ranked third, and technology factors ranked lowest. Awareness and training lead as success factors for CSRM implementation success among people factors followed by top management support. This trend was apparent by the considerable investment in awareness and training as corroborated by all and the unique approach to ensure CSRM awareness becomes every staff culture. However, two participants considered certain factors key to CSRM implementation success among the people factors. Top Management support and adequate funding are critical to CSRM implementation success because the budget may never be enough

due to the peculiarity of cybercrimes and security in Nigeria. Cybercrimes are evolving, so also management and mitigation are evolving.

Organisational factors rank second with the CSRM goals' alignment with the business goal and establishing appropriate corporate governance structure as strongly expressed in the interview by all the participants. The importance is painstakingly communicated in developing the CSRM framework for all DMBs and PSBs and adapting the C2M2 maturity model. These two support the ongoing development, strengthening organisations' CS capabilities by sharing knowledge, best practices, and relevant references/collaborations across organisations both local and abroad to consistently evaluate, effectively improve and benchmark their CSRM capabilities.

Corporate Governance has provided the direction to the implementation of CSRM with the CSRM group responsible for driving the adopted CSRM programme and compliance with processes, policies, and procedures within the organisation and by extension as a regulator/supervisor of other DMBs and PSBs. Hence, the departmental managers' accountability is considered key to CSRM success since the organisation is a role-based organisation with the core CSRM functions divided into different units. Moreover, although the organisation leverages existing and new technologies to help in their CSRM programme, there seems to be more collaboration with other key departmental heads and the dedicated staff in the CS programme.

Next, other success factors were identified by the participants as discussed.

5.3.5.7 New Factors Identified

Six new factors identified are change management, departmental staff accountability, collaboration with other organisations, defined roles and responsibilities, law and regulations, response time and performance measurement, as shown in figure 5.24. They were later grouped into the existing major categories.

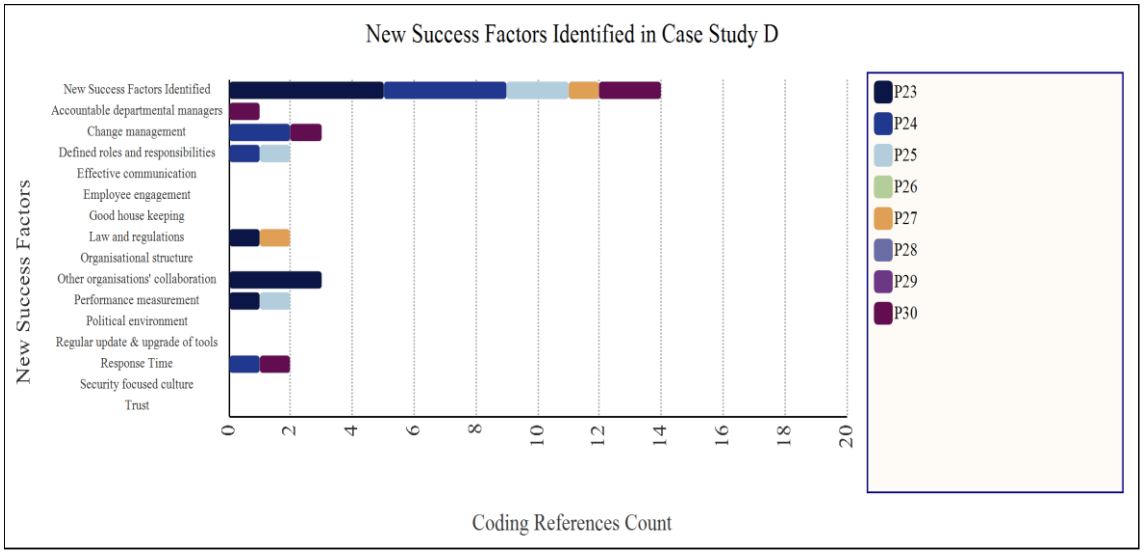

Figure 5.24: New Factors Identified in Case Study D

Figure 5.24 highlights the new success factors identified and subsequently discussed. Case study D is a role-based organisation in its bank and regulatory institution operations. As a regulator, the first and most important aspect of the CS framework is to prescribe set roles and responsibilities for the stakeholders (herein referred to as PMBs and PSPs), of which non-compliance is acceptable. Likewise, the bank's operations team acknowledged that the significant factor affecting the CSRM framework's implementation is management support and department managers' accountability. Hence, the apex organisation prescribed CISO/ISO appointment with full CS function in all the financial institutions as one of the primary prerequisites to successful CSRM implementation.

Collaboration amongst the financial industry, both local and international and other industries like the telecommunications industry and law enforcement, is necessary for the latest developments in the CS domain and share experiences while learning from one another. For example, all-time security monitoring and incident response, resilience, disaster recovery and the development of forensics (digital evidence) in CS incidents. The inputs from the collaboration with the stakeholders lead to high compliance with the new framework.

Performance measurement is identified as one of the key success factors of the bank. Assigning a set target and response time to priority areas of each unit within the organisation. Such performance factors include vulnerability management and up to date patches. For example, within 30 days, a target is set for controls to identify high and critical vulnerabilities to prevent

occurrence. The stakeholders' performance is directly linked to the effectiveness of the institution's regulatory/supervisory arm.

Establishing functional legal systems where CS cases can be treated and prosecuted cybercriminals is imminent. As of date, the legal system in Nigeria is fragile, with very few forensic experts. There are no laws for CS to deter cybercriminals, but an imperfect CS Act, was passed in 2015, and the enforcement agents need the training to understand what CS is.

5.3.5.8 Summary of Case Study D

Case study D thematic analysis revealed that using the C2M2 model at level four for financial institutions strengthens the organisation's CS capability. It improves vulnerability, defence-in-depth protection for all security assets and achieves CSRM success for the institution and its stakeholders across ten domains.

The institution's management steered by the CS strategy group used change management and extensive periodic awareness and training programmes of all staff, including the Board, to manage the eight key CS risk areas across these domains. These domains range from (1) targeted internal threat intelligence through targeted cross-platform user activity monitoring; (2) security event monitoring of internal and external threat intelligence correlation; (3) asset protection, regular business drills in readiness for cyberattack preparation;(4) targeted intelligence-based cyber awareness and training programmes; (5) behavioural analytics using workforce or customer behavioural profiling; (6) external threat intelligence of hacker or criminal surveillance through threat intelligence collaboration within financial, telecoms and government sectors both national and international; (7) manual and advance threat hunting, malware discoveries with advanced new technologies (artificial intelligence) and (8) forensics and brand monitoring.

The success factors for CSRM implementation identified by the operations and the regulatory staff representing the top and lower management, technical and network staffs interviewed were categorised into four main themes- Organisational, People, Process and Technology factors and 14 sub-themes (factors). Cyber security knowledge through awareness and training challenge CSRM implementation failures/success (Tisdale 2015). Regular awareness and training for all staff are the most influential success factors that heighten top management support and investment and drive the CSRM implementation phases.

One of the organisation’s overall implementation success measures is using the C2M2 model discussed above.

The CSRM implementation is deemed successful by most of the operations and regulatory staff interviewed. Nevertheless, a top network staff thinks more room for management improvement. There is a need for investment in state-of-the-art technology for expert intelligence detection of threats, forensics, acquisition, and retention of more expert CS staff. Also, the enactment of CS laws and acts to prosecute and deter CS criminals is unavailable to make CSRM much more successful as a bank and an apex regulatory/supervisory institution in Nigeria.

5.4 Chapter Summary

This chapter analysed and presented the success factors for CSRM implementation in the four case studies, namely Case studies A, B, C and D. Empirical data was collated from semi-structured interviews and organisation review documents. The data collection provided insights and understanding of CSRM implementation's factors validated the conceptual model proposed in Chapter 3 using thematic analysis.

The data received were collected until there was sufficient data to validate the proposed success factors model, besides the new factors identified during the interview process. Data were grouped into themes and analysed following the categories identified during the literature review findings to understand the significant activities' success factors. The data collected from the four case studies were comparatively similar. All the organisations emphasized the importance of a holistic risk-based approach to CSRM implementation success.

The identified success factors have contributed immensely to the organisations' competitive business environment in achieving their CSRM implementation goals. Top management support backed with adequate budget planning with continuous, targeted awareness and training programmes mitigate the social and technological risks commonly associated with cybersecurity negligence and challenges. Corporate governance, skilled staff with IT competencies of quality technical controls such as AI and machine learning (relatively new in cybersecurity compared with other fields as suggested by Chan et al. 2019), defined roles and responsibilities are crucial in managing the detrimental impacts of cyber security risks and its implementation success.
Concluding this chapter, a within-case thematic analysis assisted in producing case study reports from the four organisations reviewed by the interviewees as suggested by (Yin 2018). The next

chapter presents the subsequent cross-case analysis, which compares the within-case findings for commonalities and key differences.

Chapter 6: Comparing Case Studies Findings and Discussions

6.1 Introduction

The overarching research question was: What success factors impact CSRM implementation in large organisations in Nigeria? Subsequently, consider the research questions (section 1.6). Next, the following research objectives: (a) the success factors that influence CSRM implementation in the case organisations identified as a gap in the literature review, (b) Identification and development of a model of success factors that influence CSRM implementation success in large organisation evidenced by the participants' responses.

This comparative analysis and discussion aim to examine those success factors within the four case studies influential in the successful implementation of CSRM, as mentioned earlier in this study. Semi-structured interviews were conducted on a purposively selected sample of four large organisations; participants cut through the top-down management levels. Responses gathered through the interview protocol were separately analysed in NVivo software through thematic analysis. Several prominent and unique themes emerged. The themes are (a) People factors, (b) Technological factors, (c) Process factors, (d) Organisational factors. Various sub-themes under these themes have appeared in the literature review—the analysis of each case presented in the previous chapter.

The comparative analysis of the four cases provided in-depth knowledge and a clear understanding of how these success factors can enhance successful CSRM implementation in large organisations and small businesses. The detailed findings from each case study agree with the diverse experts' opinions and views from the top management, mid-management, technical and operations staff of that organisation. Therefore, the comparative analysis provided how the factors addressed the organisations' benefits and the associated values of CSRM implementation in the four case studies.

The qualitative analysis findings from the four cases from the overall combined perspective were compared simultaneously under each section themes and sub-themes to present the patterns, similarities, and differences in the success factors for CSRM implementation across the four case studies. The comparative analysis provided comprehensive findings that could help other organisations' top management and key staff implement CSRM successfully.

Figure 6.1 illustrates the thematic template of themes and sub-themes, showing the success factors for CSRM implementation for each case study.

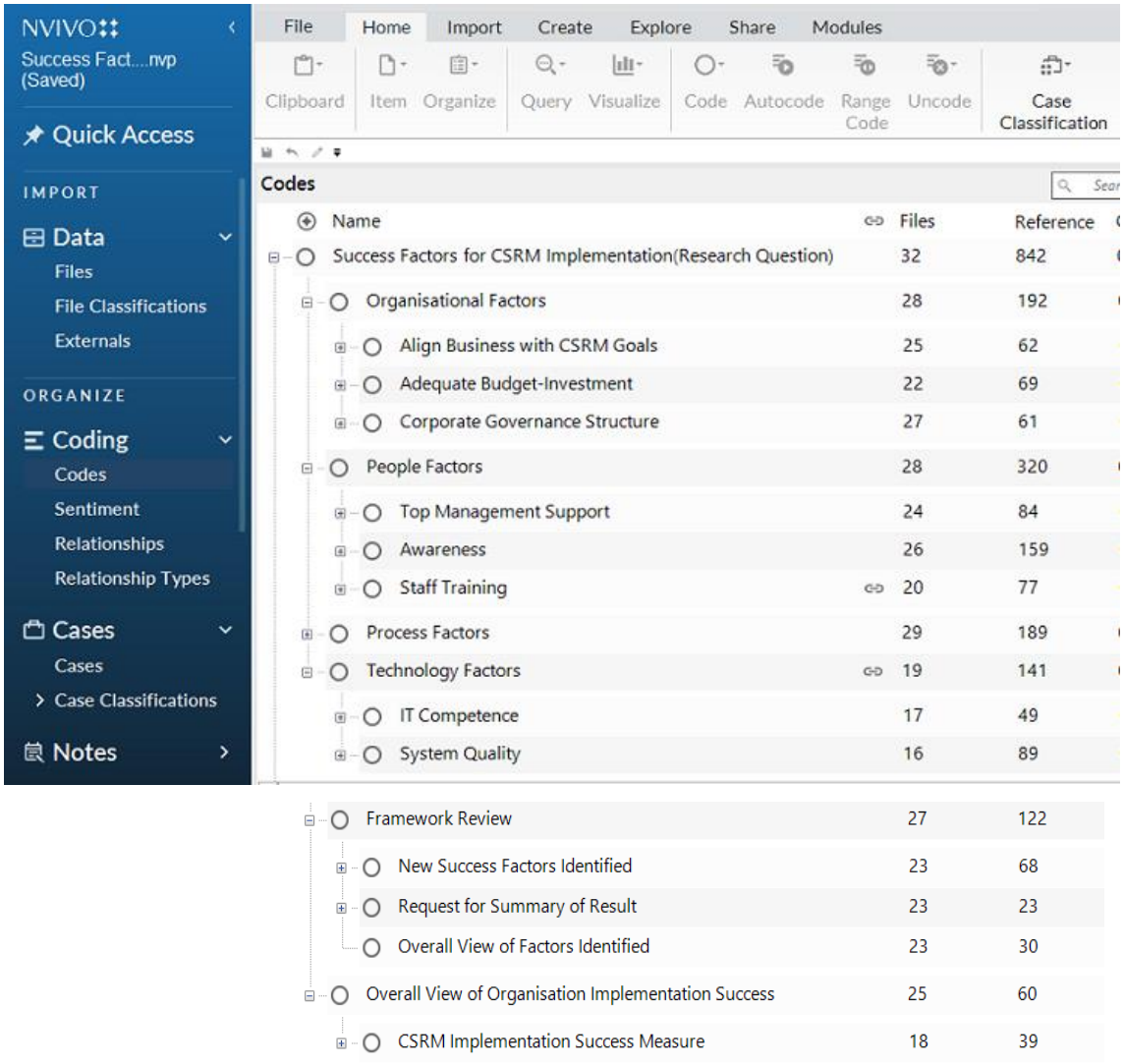

Figure 6.1: Combined Thematic Template of the Themes and Sub-Themes

Figure 6.1 illustrates the template for each case study which includes the success factors for CSRM under the four major themes and the sub-themes adopted for CSRM. The new factors identified, the framework review and the overall view of the organisation's CSRM implementation success as perceived by the participants.

6.2 Overview of the Comparative Case Studies

The within-case analysis of the case studies discussed below is summarised in Table 6.1 below.

Table 6.1: Overview of the Comparative Case Analysis

Unit of Analysis	Case Study A	Case Study B	Case Study C	Case Study D
Company activities	E-retail	Financial industry	Financial industry	Regulatory industry
Years of operation	≥5 years	≥30 years	≥25 years	≥100
Number of employees	≥1000	≥1000	≥1000	≥1000
Geographic spread[2]	West Africa	Multinational	Anglophone West African and United Kingdom	Nigeria
Approach to CSRM	Proactive	Mixed (Proactive + reactive)	Proactive	Mixed (Proactive + reactive)
RM Model	PDCA (Mixed-ISO 27001+NIST+PCI-DSS) (Risk-based approach)	Mainly CSRM framework +ISO 27001, PCI-DSS (Risk-based approach)	Mainly CSRM framework +ISO 27001, PCI-DSS (Risk-based approach)	Mainly C2M2 +CBN framework, PCI-DSS, ISO 27001 (Risk-based approach)
Ownership of CSRM	Top management	Board	Top management/Board	Board, functional unit role-based
Awareness approach	Aggressive (majorly staff centric)	Aggressive (Staff And customer-centric	Aggressive (Staff and customer-centric)	Aggressive (stakeholder +staff)
Awareness medium	Mainly digital	Digital and face-face /yearly roadshows	Mainly digital, yearly CS week programme (Digital)	Digital, face-Face
Training medium	Mainly digital/on-boarding face-face, employee engagement, case studies	Mixed (face-face, departmental, digital	Mainly digital/on-boarding face-face, case studies	On-boarding face-face, departmental, International conferences, collaborations community-groups, case studies, colleagues
Top management support	Very high	High (but took years to buy-in)	Very high (Proactive)	Very high (took little time to buy-in)
IT competence	Very high	High	Very high	High
System quality	High	High	High	High
Corporate governance	CISO, Risk manager, Security Engineers, Legal, Board	CISO led team, CRO, Board (operations, audit &control)	The steering committee, CISO, compliance teams, auditors	CSRM strategy group (critical departmental units), Board

[2] Geographic spread denotes the various locations and regions where each case study organisation has branches in operations. This shows how large these organisations are. Please note, this study does not pre-suppose that the empirical research took place in other regions but in Nigeria (the head quarter of all the case organisations).

Budget/Investment	Adequate	Somewhat adequate	Adequate	Somewhat adequate
CSRM policies compliance	High	Somewhat high	High	High
Security audit	Internal &external	Internal &external	Internal &external	Internal &external
Rate of CSRM success	70%	70%	80%	≥70%
The measure of CSRM maturity level	Six sigma	KPI and as defined by CBN framework	KRI/KPI and as defined by CBN framework	C2M2
Key CSRM values	Tremendous confidence in partner engagements, CSRM maturity as selling point /customer satisfaction	Sustains reputation damage and customer loyalty	Tremendous confidence in partner engagements, CSRM maturity as a unique selling point, colossal customer satisfaction	High-level maturity at Level 4 of the C2M2 model typical of a regulatory/Apex institution. Huge stakeholder confidence.

Each theme and sub-themes are compared under the relevant section for the four cases in table 6.1 above. The comparative analysis is structured into four sections per the objectives and research questions of the study.

6.2.1 Theme 1: People Factors

Most efforts toward improving CSRM have focused mainly on integrating new technical approaches into processes and products. While technological solutions are a prominent feature of CSRM, a vital element of enhancing CSRM success should involve understanding how human behavioural factors can lead to more technology effectiveness and CSRM failures if personnel are unaware and lack sufficient training (Pfleeger and Caputo 2012). The people factors theme in this study refers to those associated with stakeholders possessing requisite knowledge and skills for effective and efficient CSRM functions that make CSRM implementation successful in the organisation. People factors answer research question 1:

> ***What are the People factors associated with CSRM implementation success in large organisations in Nigeria?***

The subthemes captured under people factors from participants and organisational documents with their coding reference counts are shown in figure 6.1. The identified sub-theme includes awareness, training, and top management support, discussed below.

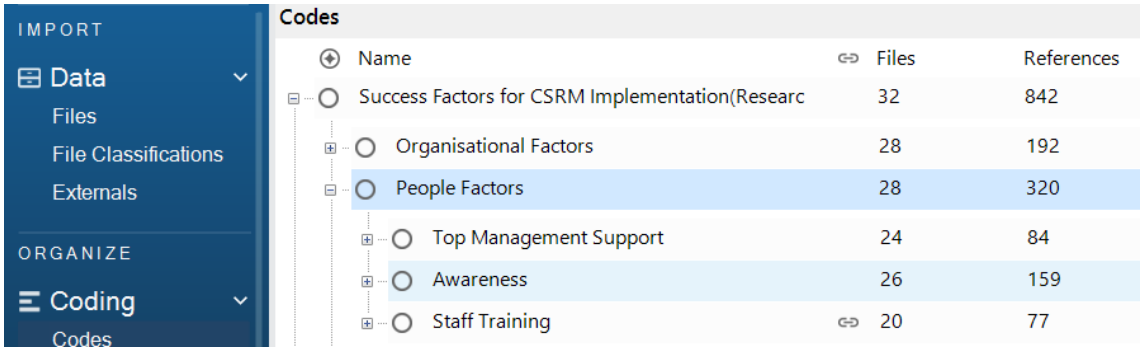

Figure 6.1: People Factor Theme and Sub-Themes

320 out of 842 reference counts show the importance of people factors as success factors for CSRM implementation in Nigeria's case organisations. People factors due diligence ensure that technological solutions prove effective despite their key feature in CSRM implementation.

- **Awareness**

In most discussions, awareness and training are interwoven and often interchanged, although not analogous. For clarity, in this study context, the concept of awareness in section 2.7.2 means all stakeholders create a shift in thinking through supporting materials, guidance and training dedicated to inspiring positive behavioural, attitudinal, and cultural change towards successful CSRM implementation.

Figure 6.2 shows the participant's responses to the initiatives to create awareness of CSRM implementation, the medium and mode of evaluation of the level of understanding gained and the effectiveness of awareness programmes in CSRM success. The medium of awareness and training means communicating the necessary information, skills, and knowledge to stakeholders.

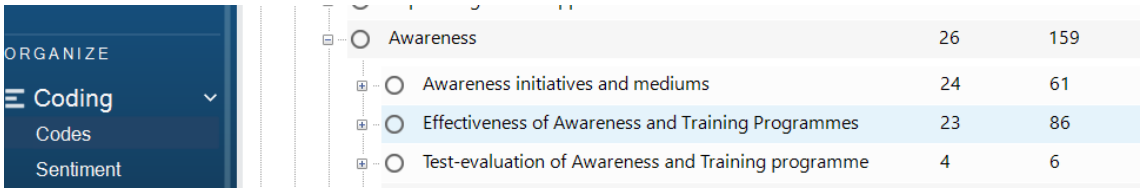

Figure 6.2: Awareness Sub-Theme for CSRM Implementation Success

Participants from case studies A, B, C and D communicate most of their awareness programmes via similar media. Such media include web posters, email, computer screen savers, monthly newsletters, bulletin boards, and more, as shown in figure 6.3.

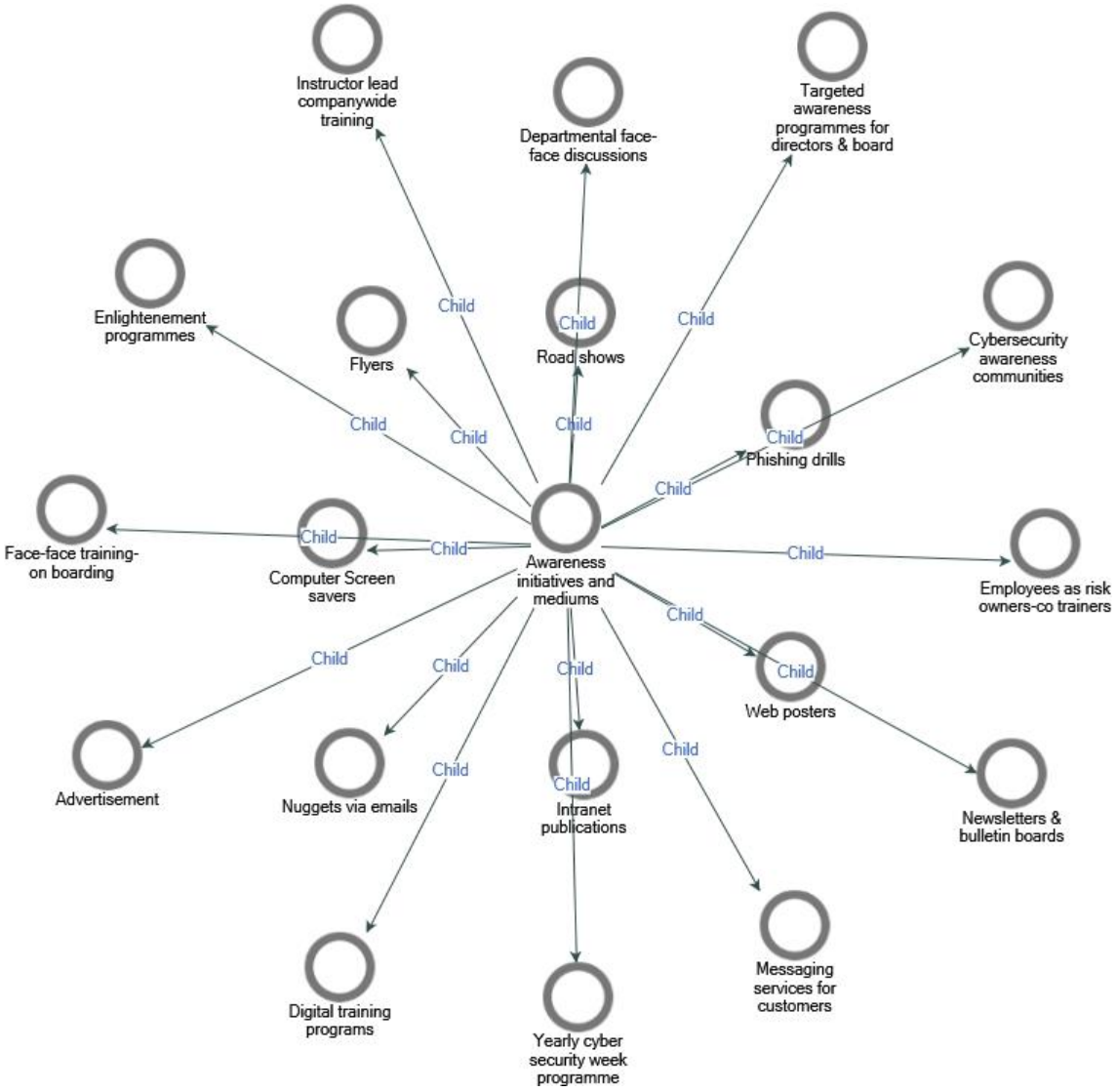

Figure 6.3: Awareness Initiatives and Mediums

All the participants expressed that CS risks and management's awareness takes a top-down approach in the organisations and is done mainly through nuggets via email. Case studies A, B, C, use digital training using videos for sensitization and training. In contrast, case studies A, C and D incorporate awareness programmes as part of the onboarding face-face training for new intakes. B, C and D use screen savers of office computers and desktops as awareness mediums.

Case studies B and C include cybersecurity awareness text messages as part of transaction alerts to customers, online accounts, fliers, and many more for enlightenment.

Case study A expressed that as part of the on-boarding face-face awareness and training programme, employees are allowed to be the risk owner - this requires the employees to be a little more creative and personal with CS training in an easy way understandable (P7). An exciting and distinguishing act is that Case study B goes a step further in engraving the awareness of CS risks and management in both staff and customers by conducting yearly roadshows. This roadshow targets creating broader awareness for the customers. Key IT staff also attend an annual community conference where experts deliver talks on CS and simulated phishing drills to create awareness.

Similarly, a yearly cyber-awareness and training week in Case study C sensitises employees on CS issues. It emphasises the importance and implementation of CSRM with a dedicated information security group portal for learning. According to P19, officers win gifts for answering questions correctly in the programme. In addition to the shared awareness medium, case study D conducts quarterly targeted CS awareness programmes for the top management and board of directors and periodic departmental sessions and presentations at other staff meetings. Other awareness media include web posters and monthly newsletters.

- **Training**

Training is a formal learning process focusing on acquiring the necessary physical skills to perform CSRM tasks, processes, and procedures with minimal effort to achieve CSRM goals and business objectives. In like manner, figure 6.4 shows the participant's training initiatives and media for CSRM implementation.

Figure 6.4: Training Platforms

Figure 6.4 shows the CSRM training platforms, although similar to awareness mediums, but with some differences. In all case studies, mediums such as nuggets, pop-up tips, computer screen savers, and emails are shared and used for CSRM training. As discussed earlier in the awareness and training section, Case studies A, B, C use digital video training. In contrast, case studies A, B, C, and D incorporate awareness and training programmes as part of the onboarding, face-face training new intakes.

Cases study A expressed that any new staff's onboarding classroom training failure within the probation period leads to appointment termination—self-learning through digital subscriptions like Udemy. CSRM policies, procedures and countermeasure training programmes form part of

the companies living documents hosted on the EDMS. The security team communicates quarterly reviews and updates of these documents using random security quizzes, emails, and nuggets.

The use of quarterly in–house onsite training and case studies of life scenarios, simulations to re-orientate users, dedicated local intranet portal with self-study materials and videos to learn about CS at spear times are part of training media to ground understanding in case study B. Also, solution providers' awareness training enlightens users of the latest security threats and the bank's solutions. Similarly, passing the onboarding e-learning courses on CS training is a criterion for job confirmation after a 6-months probation period. Key officers' subscriptions on e-learning and ISO certification constitute the major training platforms in case study C. Case study D conducts an annual round table training for top management and directors to appreciate CS.

Figure 6.5 highlights the effectiveness of CSRM awareness and training initiatives on staff capability and the value gained about CSRM implementation success in the organisations.

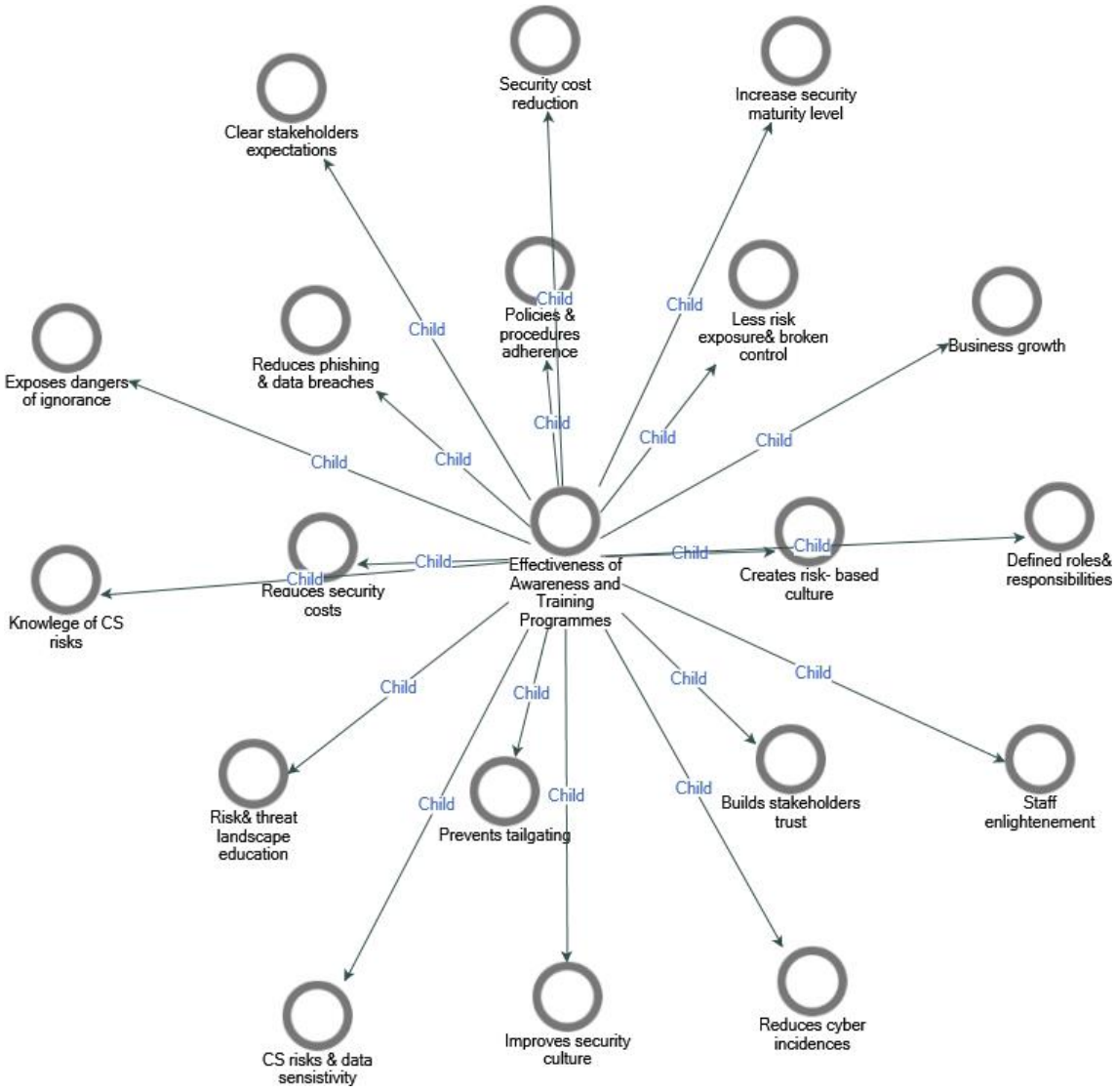

Figure 6.5: Effectiveness of Awareness and Training Initiatives and Programmes

In figure 6.5, 17 sub-themes (13 typical sub-themes and four others) show how CS awareness and training contributed to the success of CSRM implementation in these organisations. The values gained include: The increased capability to reduce phishing and data breaches because employees can now identify phishing emails/links and report more frequently; reduced uncertainties regarding cybersecurity expectations, roles and responsibilities of staff towards CSRM; education of staff and users on CS risks and threats landscape with reduced CSRM deficiencies; ensures strict adherence to CSRM policies and procedures; reduction in the number of broken controls and risk exposures as users have a deeper understanding of inherent risks in their activities and ensure adherence to the recommended controls. Embedding security culture in daily work practices through CSRM awareness and training of all staff increases the top-down security buy-

in, improves the organisations' CS risk culture and prevents tailgating. Constant CS awareness and education of the employees reduces enterprise security risk costs and financial losses.

The awareness and training sub-themes encompass the efforts made to ensure that everyone in the organisational system is aware of processes, policies, expectations, roles, responsibilities and functions in the CSRM implementation success. Further extends to knowing what to do when situations that can jeopardise CSRM implementation success arises. Analyses dispel the myth surrounding the CSRM implementation issues as a technology issue. Management of technology alone still proves an insufficient solution to CSRM success consistent with many experts (Chabinsky 2014; Soomro, Zahoor Ahmed 2016). Users are more informed and ask more questions when in doubt. Unlike the debatable rhetoric that employees are weak links in matters related to CS issues in organisations (Bendovschi 2015; Harrison and Jürjens 2017), there is no sufficient evidence to support such arguments in the four case studies. Instead, employees' capabilities have contributed to CSRM implementation success in these case organisations. Hence, previous opinions are somewhat weak and unconvincing.

Awareness and training resonate among most participants as key success factors for CSRM implementation. Magic happens at CS awareness and training workshop sessions through interaction with people (Mikes and Kaplan 2014). A top-bottom approach to training and awareness with technical best practices, appropriate technology, technological know-how or skills, responsible behaviours in handling technology will promote cyber peace (Shackelford 2016; Shackelford et al. 2015.

According to the findings, awareness and training ranked second as success factors for CSRM implementation. This ranking confirms that having the correct information, effective communication and requisite knowledge, skill and education through awareness and training programmes will lead to the desired change in people’s attitude and behaviour towards CSRM implementation success. Risk management tasks, appropriate use of tools and technology, CSRM controls, policies and procedures will be much more effective and adhered to by stakeholders resulting in a more successful CSRM implementation process.

Finally, participants evaluate the effectiveness of training and awareness. Case study A uses a balanced scorecard report integrated on the SIEM platform to review any significant occurrence within a specific time of the year. Case study B uses participants' feedback responses. In contrast, Case study C uses phishing emails to determine staff's vulnerabilities, evaluation surveys by

supervisors three months after training and internal audits, social engineering test and percentage failure on the e-learning platform. Case study D conducts phishing exams after training for evaluation. However, a staff's failure multiple times does not lead to appointment termination, unlike case studies A and B. Still, a call on experts or knowledgeable colleagues to have a physical discussion with those that failed to put them through. Also, Case study D uses the adapted C2M2 model to determine CSRM maturity within the organisation at level four for financial institutions prescribed by the US Department of energy.

- **Top Management Support**

The previous section, 2.7.2, defines Top management support as unwavering commitment, dedication, and leadership to achieve CSRM implementation success. Top management support is ubiquitous in many success factors research in organisations (Hu et al. 2012; Yaraghi and Langhe 2011). It is impossible to discuss or examine CSRM success without reference to Top Management support.

Various explanations have been put forward in the literature. For example, top management's perception ensures integrating CSRM requirements into the organisation’s processes and procedures. The implementation of CSRM policies, controls and compliance by all employees and allocating sufficient human and financial resources for CSRM implementation success. These are possible when top management understands how CSRM implementation success supports the core business functions.

Figure 6.6 below shows some of the participants’ comments on top management's effectiveness supports CSRM success sub-themes.

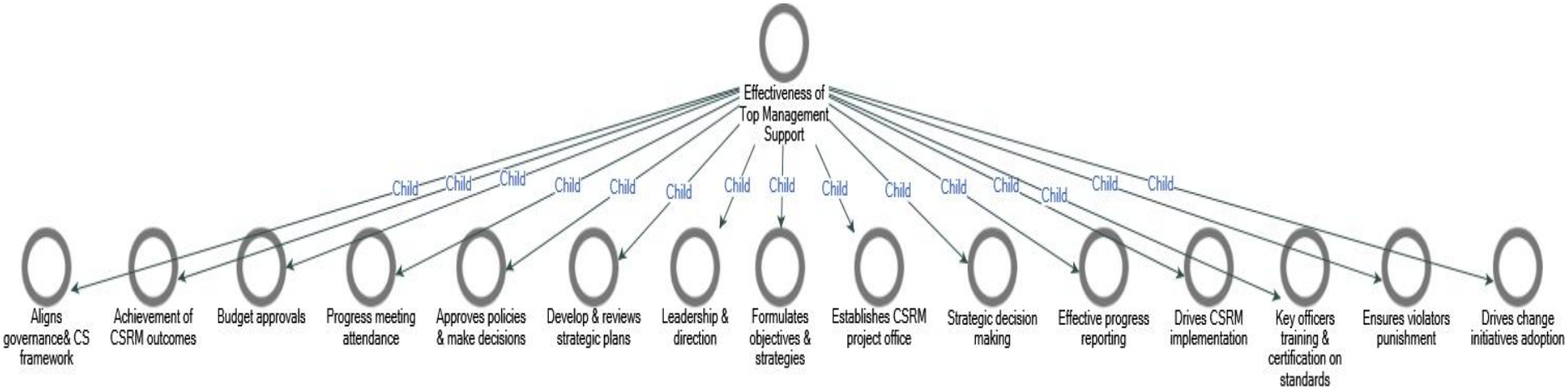

Figure 6.6: Effectiveness of Top Management Support

Figure 6.6 above shows the effectiveness of top management support in CSRM implementation success is further compressed into eight sub-themes and discussed:

1) **Leadership and direction**:

In case study A, ***Top management support is critical to*** *CSRM implementation success as top management* ***drives*** *the implementation of the policies and most of the budget are to be approved by them. So, the buy-in by* ***leading*** *and providing necessary support (P5). CEO severally emailed all staff to remind them of their security responsibilities in case study B (P11). Top management provides* ***strategic direction*** *through the approval of policies and procedures regarding CSRM (P18); the fact that the executives* ***participate*** *in user awareness programs goes a long way to get the buy-in of staff's generality in case study C (P21). Case study D affirms all the submissions that the tone at the top is an essential ingredient to CSRM success. Tone at the top is critical in our organisation; if top management supports the cause of CSRM, then the compliance level will increase corporate-wide (P29).*

2) Ensures that enterprise governance is aligned with the cyber/information security governance framework to achieve the intended outcomes. A participant from case study A comments; *Top management also ensures* ***alignment*** *with business strategy to meet the organisation's* ***strategic objectives. A CSRM program identifies and mitigates the impacts on*** *an organisation's resources and assets (P1).* Hence, case study C concluded that ***without top management support,*** *it would be challenging to implement a CSRM (P18).*
3) *Top management formulates and decides objectives and strategies for organisational risk management activities to predict the likelihood of a negative impact (P6).* They engage with the CS manager to help prioritise information assets and make specific trade-offs between risk reduction and operational implications. All participants mentioned budget approvals to get the tools and resources needed for CS and effective and efficient resource management. *They also approved the budget for training and certification of officers on ISO standards (P21).* Perhaps this paved the way for the high success claim in CSRM in case study C.
4) Establishes the CSRM project management office and puts effective, granular reporting on how the company progresses against specific milestones in its CS program through timely and useful metrics reporting (4).

5) Top management helps span CS implications across business functions, pushing changes in user behaviour. *Top management provided the communications channel and reinforcement required to help frontline employees understand what they need to do to protect critical information assets (P16).*
6) During policy development and ensuring staff comply with the policies and processes put in place within the organisation. *Top management helps drive this implementation process by sending emails to all staff to comply with other punishments on erring employees (P19).*
7) *Develop, follow up and review CSRM strategic direction and policies by asking for a CSRM road map yearly and providing value-added information security initiatives (P 1).*
8) *They have been supportive, considering the CS environment and ensuring that employees are aware of CS and put security measures on violators (P12).*
9) Although, initially it took some painstaking efforts to explain the need for much investment in case study D, the institution, as a regulatory/supervisor and an epitome of top management support, *decides and organises training, workshops, and conferences necessary to advance CSRM awareness and success both locally and internationally for all its stakeholder organisations (especially the CISOs) (P27).*

All these comments from the participants have benefitted and supported previous studies that top management support is vital for CSRM implementation success in most security/information success factors studies (Chatterjee 2019, Kikwasi 2018). Top management support (figure 6.6) builds adequately aware and well-trained staff through several media (see figure 6.3 and 6.4). Thereby leads to an overall risk-based culture that increases CSRM implementation maturity and eliminates the dangers of ignorance (Kennedy 2016). Figure 6.5 shows the positive outcomes at the organisational level.

In agreement with the literature, CSRM implementation activities efforts to raise awareness and training in CSRM fall in line with risk management processes/phases (section 2.5.1). The banking professionals have earned sufficient awareness and training through management support (Alawonde 2020; Wang, Nnaji and Jung 2020). The successful CSRM implementation can be achieved through technical solutions, management support and people factors (Rhee, Ryu and Kim 2012). This assertion is supported and summarised in the words of P20:

Another factor that impacts the success of CSRM is people risk. While Technology solutions are essential in protecting organization vulnerabilities, the human factor cannot be overlooked.

Cybersecurity risk management initiatives need to be driven, supported and implemented by agile, competent, motivated and aware people (Maarop et al. 2015). Therefore, recognising people factors as success factors for CSRM is necessary and thus answers research question 1.
Having established the people factors above, the behaviour and taxonomy of threats to CSRM, Technological success factors are companions that provide the means to neutralise the technology threats, maximise people factors and facilitate CSRM implementation success.

6.2.2 Theme 2: Technology Factors

Technology facilitates task (process), people and organisational dimensions in social-business transactions and relationships (Coiera 2007). Technology factors include the body of technologies (tools and resources (hardware and software, tangible, and intangible), designed to facilitate the protection of security assets and used to accomplish CSRM work activities.

Technology factors answer research question 2: the participants acknowledge technical factors as success factors for CSRM implementation but with diverse opinions. Three participants from case study B expressed that non-technical factors (i.e., people factors) are much more critical than Technology factors because technology will only perform at its best by eliminating challenges of human factors. On the contrary, others considered technology factors as a means of control to prevent human failures. Therefore, Technology mediates between people within an organisation's business-functional context.

> ***Theme 2: What are the Technological factors associated with CSRM implementation success in large organisations in Nigeria?***

Such technology factors for CSRM implementation encapsulates the identification of two sub-themes: system quality and IT competence.

- **IT Competence**

IT competence is conceptualised as the combined knowledge and skills embedded in people and technological resources' complementary capabilities to consistently fulfil its business objective. Realising that CS risk is becoming more sophisticated and seems inevitable in business, in-depth knowledge of information systems and risk management is essential (Hoffmann, Kiedrowicz and Stanik 2016; Webb et al. 2014).

The participants shared how staff's IT capability, both inbound and outsourced, helped achieve CSRM implementation success in their organisation with the various technical solutions developed. Case study A participants explain that the **IT team** comprises **subject experts** in all areas with **many skillsets**. Furthermore, the CISO, with 20 years of experience, commented that 'the major concept in achieving a risk-based CS management system revolves around **People, Process and Technology** (Highlighted for emphasis based on the tone of the conversation). Technical control is a major part of CSRM implementation. The **IT team can deploy systems** through internal and outsourced resources to deploy encryption, antivirus software, IDSs (Intrusion Detection Systems), firewalls and the principle of least privilege'. The principle of least privilege is when users have limited access rights to the barest minimum permissions they need to perform their duties as a safety net irrespective of the training and awareness education programme (Fielding and Security 2020).

The participants also explained that their staff's IT competence, especially in ensuring regular awareness and training via several media, has helped the entire staff be IT literate and imbibe the necessary CSRM culture in their operations. Below is a comment from P4:

> *Regular awareness* and *training, to some extent, helped a lot because most employees are **IT literate** and have been able to **identify phishing emails and other potential threats.***

.

In contrast, case study B participants' opinions of IT competence differ significantly from case study A. For example, P14 comments:

> *The most effective deterrent to cyber risk is good housekeeping. In most cases, it does not require advanced technical skills to achieve. Though technology is why we have the term cyber before the risk element; Technical skill is not a significant concern; Cyber-risk awareness is more crucial in CSRM implementation success*.

However, the recruitment phases consider the IT competence factor - the staff's ability to have above-average ability to work with technology. Hence, P10 believes **Technology helps 20%-** because the system quality and the capacity to perform well is directly related to human factors. Whereas, in case study C, IT competence is considered a success factor for CSRM. **IT capability of staff** has **helped a great deal** as accomplishing **CSRM implementation success has come**

through their capacity (P20). Individuals with a **good understanding of the requirements of CSRM** help **ensure CSRM implementation success** (P18).

Likewise, in case study C, having a skilled and dedicated IT/CS staff is at the core of their CSRM programme. According to P23, **dedicated and committed staffs are** in **their CS programme**. Coupled with a background check to ensure that only staff with administrative access work in the CS team. These analyses show that in case studies A, C and D, the primary task of CSRM implementation rests with the IT/CS and the risk management team. While case study B believes that developing user capacity is much more desirable than building/relying on the IT competence of some selected IT professionals. However, threat identification, assessment, deployment and implementation of necessary controls and mitigation activities require competent teams.

Furthermore, the participants highlight how they measure that IT end-users follow the sound process, knowing that CSRM is not just an IT staff issue. Case study C uses various techniques such as periodic conduct of awareness test and unannounced data security sweep, enforced controls through a central-managed technology, and usage logged using a SIEM. A weekly measure of systems without up-to-date patches and antivirus conduct reveals the number of vulnerable end-users, thereby showing compliance with set CSRM operational rules.

On the contrary, Case study A uses the strict measure of penalty to enforce compliance with sound operational processes. P1 comments:

> *We **do not measure** whether end-users follow sound CSRM operation processes; we enforce them **with technical controls**. Microsoft Enterprise Mobility Suite (EMS+Security) is one product that helps control user interactions with the enterprise.*

Since case study B's views concerning IT competence in CSRM success differ somewhat, the approach differs. Some participants explained implementing synchronised security measures such as **end-to-end security to monitor, control and protect** systems' users. There is no BYOD. Hence, many end-users follow acceptable use procedures, although a few defaults occasionally.

Case study D, as a regulator, prioritises educating all staff regarding how to protect data irrespective of their background while using appropriate technologies for defence-in-depth within the organisation’s network by the dedicated team of security staff.

Figure 6.7 below shows the effectiveness of IT competence.

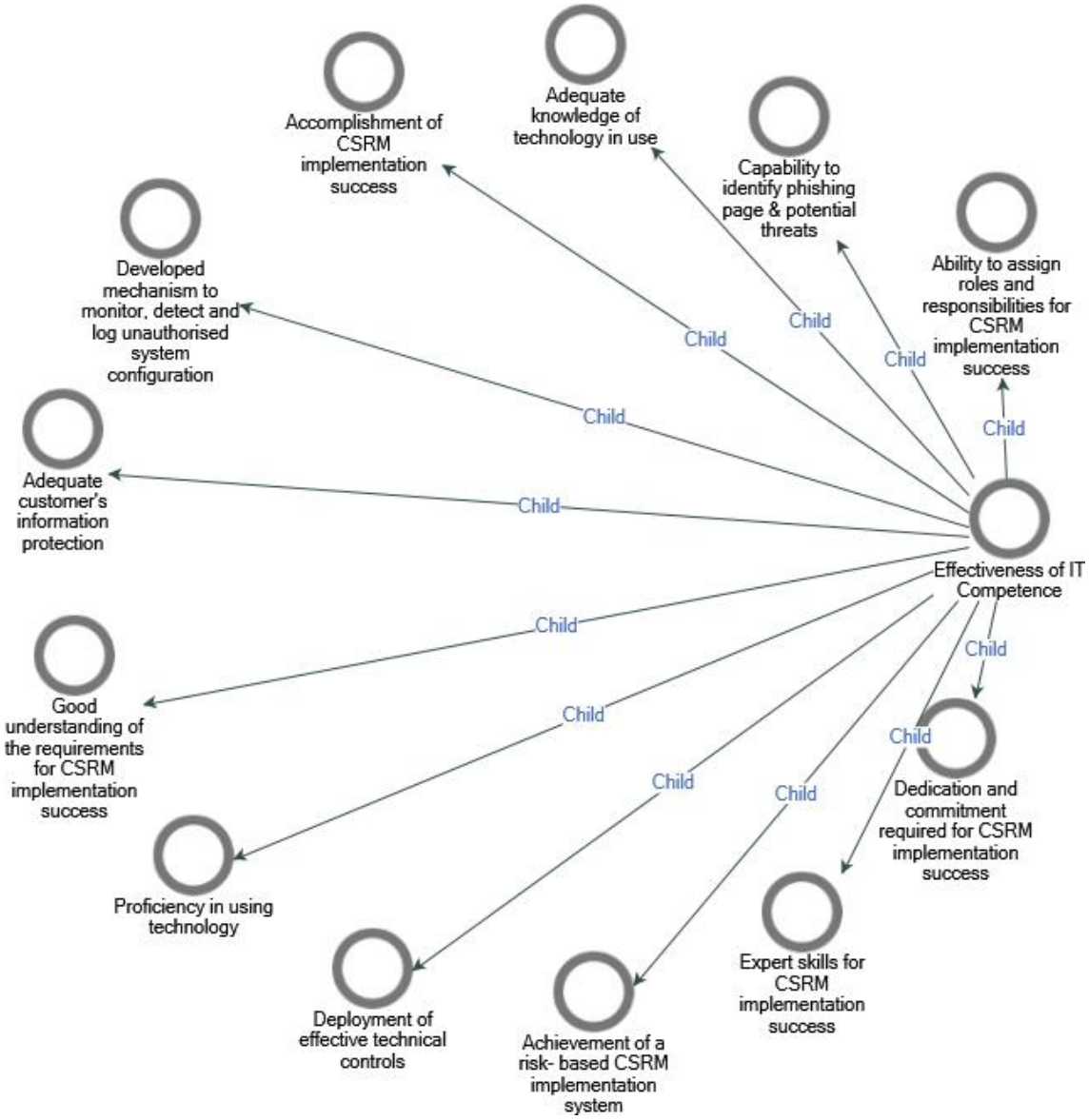

Figure 6.7: Effectiveness of IT Competence on CSRM implementation Success

Based on the above findings shown in figure 6.7, by induction, the implementation of CSRM processes needs to be supported by knowledgeable and skilled IT personnel with IT systems that enable the successful management of the processes. Case study A to D has a team of dedicated technology experts who are the primary implementer of CSRM. Therefore, IT staffs are competent in using appropriate technology to achieve CSRM implementation success. Thus, the organisations' management ensures that a proper budget is allocated for technical resources and

human resource IT capability training. This aligns with the literature that the availability of knowledge bases improves the use of technology (Kisling 2006). People's skill to operate, use or adapt appropriate technology to CSRM implementation will lead to CSRM implementation success (Lyytinen 2008).

- **System Quality (Task –Technology Fit)**

In this study context, system quality refers to the availability and reliability of the technology used for performing CSRM tasks (Palvia, Sharma and Conrath 2001). The system's quality is associated with the features of functioning and performance related to the CSRM implementation. Cybersecurity risk management integrates into nature, so the systems used for CSRM tasks are integrated into nature, making it essential for the business organisations' successful CSRM operations and processes.

The participants' opinion is that system quality is an essential technical factor that had a tremendous impact on the perceived success of CSRM implementation. The exploitation of the investment in up-to-date technology giving rise to quality systems for CSRM is deemed beneficial. If the systems' quality is not up to the expected security level, achieving organisational and CS goals for competitive advantages may be an exercise in futility.

Case studies A to D are like-minded to a great extent in their approaches to CSRM in terms of quality of systems for CSRM implementation. The participants' responses show the quality of systems (technology tools and techniques) adopted for CSRM implementation. The list of tools and techniques used is exhaustive but managed to mention a few, as shown in figure 6.8.

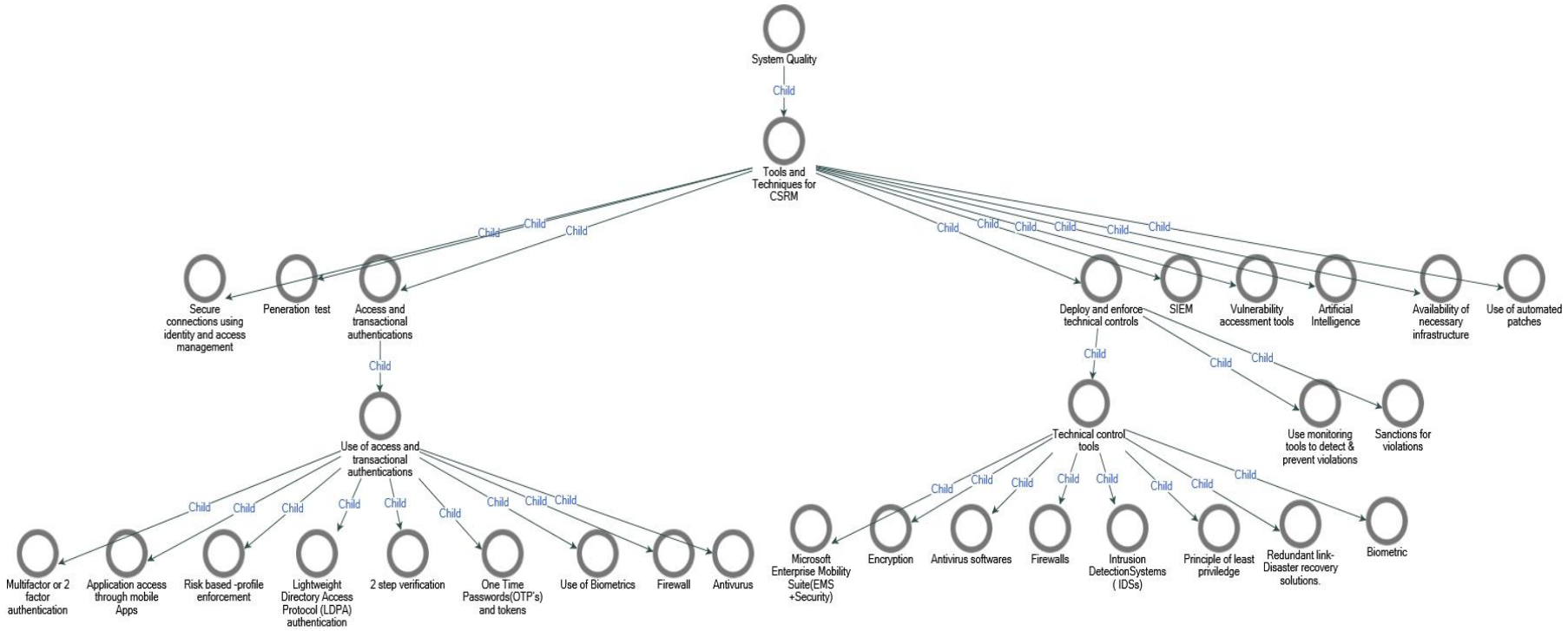

Figure 6.8: System Quality (Tools and Techniques for CSRM)

Figure 6.8 shows the system's quality used for CSRM implementation success in the case organisations. This consists of combining all the tools and techniques used for CSRM. Some technical success factors include a defence-in-depth strategy for in-depth and multi-level security protection and management and several authentications and authorisation granular access controls for cyber/ information security at different sensitivity levels as deemed fit.

Case Studies A-D assesses system quality based on the quality of the technical controls. Since CSRM is highly necessary, particularly in these sectors, they all have similar technical controls. Examples of some of their comments are:
P2, from case study A, comments that:

> O*rganisations worldwide are trying to keep up to speed with endpoint security developments by ensuring they have* ***the best infrastructure*** *to handle their data security threats.*
>
> Hence,
>
> *Having* ***quality systems*** *have been effective in many ways. It is one thing that the user is enlightened; another thing is that quality infrastructure with excellent CS measure is available to isolate any system in case of any attack for a particular day (P13)*-case study B.

P18 from case study C agrees that system quality is essential in the success of CSRM in his comments:

> ***These technology solutions*** *have had* ***a tremendous impact in protecting*** *these assets as they enforce the controls* ***even when users do not****.*

Case study D, without any exception, P23 said:

> *We do not rely on one layer of defence to ensure* ***our systems' quality****; we apply* ***various protection levels*** *to all our information assets in different layers. So, we do defence-in-depth; if one layer fails, the second and third layers may not fail.*

The few technical tools and techniques mentioned include Security Information and Event Monitoring (SIEM), which correlate security incidences and events across all platforms. Microsoft Enterprise Mobility Suite (EMS+Security) is one of those products that help control user interactions with the enterprise; vulnerability assessment and detection tools, artificial intelligence, firewalls, and encryption help CSRM organisations.

For access and transactions and authentications, multifactor, 2-factor authentication, 2 step verification, Risk-Based conditional access based on profile enforcement, Application access only through managed Apps, One–Time Password and biometrics. Case study D is a regulatory institution; unlike customer-facing organisations, the use of transactions and authentications were not discussed. However, it continually encouraged the stakeholders (DMBs and PSPs) to enhance the availability and reliability of technical security solutions by enforcing access and transaction and authentication solutions with their customers. Also, case studies A-C participants believed top management had provided necessary technological tools for CSRM. However, a participant from Case study D opined that there is a need for more updated information and acquisition of available state of the art technology as technology advances to be on top and at par with the rest of the international world. That seems a tall order, but achievable as cybercriminals are unrelenting, business leaders must also strive to achieve CSRM success.

Figure 6.9 shows the effectiveness of the system quality in the case studies.

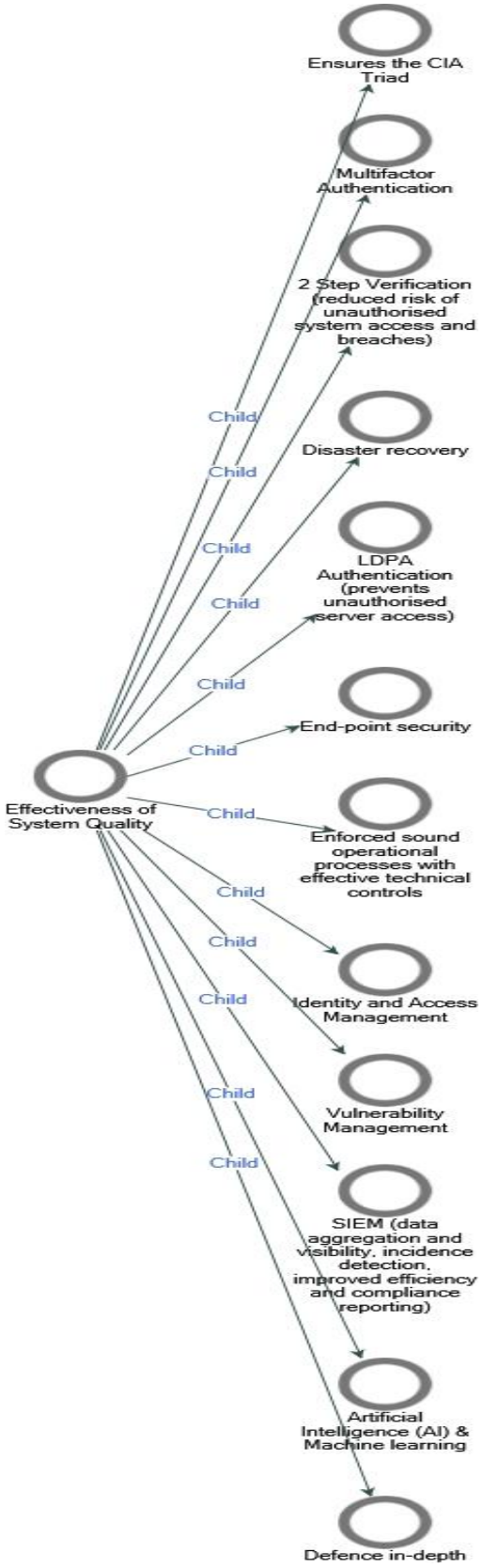

Figure 6.9: Effectiveness of the System Quality on CSRM Implementation

Security of the CIA of information and processes (transactional and access authentication) is at the heart of these organisations due to the volume of customer information and transactions. The literature identifies the advancement and use of information technology systems as a significant cause of cyber security risk (Dubois et al. 2010; Saleh and Alfantookh 2011). Simultaneously, technology is needed to drive business to balance technological risk exposures using process, procedures, and controls.

System quality involves ensuring that state-of-art information technology systems and risk management practices are available and reliable for CSRM functions. The implementation of defence-in-depth prevents and protects cyber exploitations and human vulnerabilities. The findings suggest that for successful CSRM implementation, deploying the best quality technological systems is needed for the best quality performance. However, the deployment and implementation could not have been achieved without competent IT personnel with requisite skills, knowledge, and understanding of risk analysis and management strategies and methods, as evidenced in figure 6.7. This process is achieved by ensuring that IT staff are trained and certified in all areas related to CSRM implementation success.

In summary, Figure 6.9 shows that Technology factors have shown to be influential success factors for CSRM implementation as companions to the use of security/information systems by their design, use and effectiveness. The technology factors effectively control and avert the diverse technology and multiple failures in human threats at different CSRM implementation phases. The importance of technical factors as success factors for CSRM implementation is that only one case organisation has experienced one cybersecurity breach in the last five years.

These show that comprehensive security standards and technologies link the high-level business requirements of CSRM in today's dynamic socio-technical business organisations. Thus, the finding supports the literature that Task-technology fit is an essential construct in security success (Petter, DeLone and McLean 2013). In-depth knowledge of information systems and risk management is inevitable in CSRM implementation success (Hoffmann, Kiedrowicz and Stanik 2016; Webb et al. 2014). Although most participants agree that System quality affects CSRM success performance, very few opined that CSRM success has no direct link with system success. Thus, the finding is with mixed feelings, as such should be treated with caution.

While CSRM implementation is critical, good education and understanding of the threat and possible risks landscape, infrastructural networks through skills upgrade and update knowledge,

and appropriate tools ensure CSRM implementation success. Therefore, technical success factors would provide the available and reliable means by which the security/information infrastructure and information systems facilitate the protection of the security assets for CSRM success (Dunkerley and Tejay 2011; Petter, DeLone and McLean 2013).

6.2.3 Theme 3: Process Factors

The process factors represent various risk management tasks of identifying CS risks, executing quantitative analysis and qualitative analysis, formulating and communicating risk responses, monitoring and controlling CS risks and managing CS in organisations. The process factors answer research question 3:

> ***What are the Process factors associated with CSRM implementation success in large organisations in Nigeria?***

These include the process of risk management and controls for managing CSRM implementation success, as shown in figure 6.10 below.

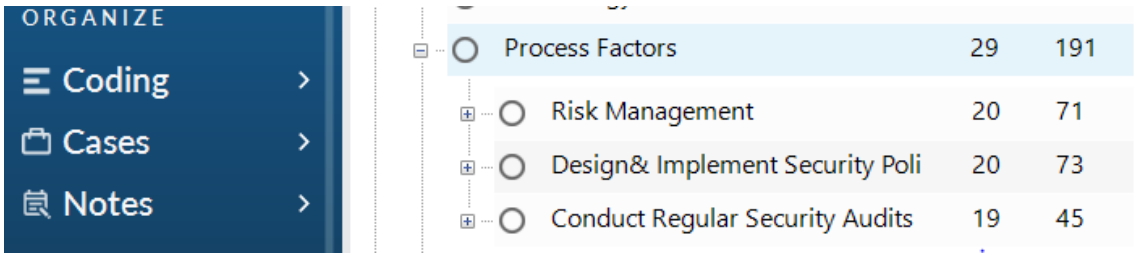

Figure 6.10: Process Factors Theme and Sub-Themes.

Figure 6.10 shows the identified sub-themes, Risk management, CSRM policies and Security Audit. Participants' responses on the themes are further discussed.

- **Risk Management**

This study defines the Risk management process as a set of principles, supported by a structure/framework that raises the awareness to identify and manage threats and emerging risks in the process throughout the organisation by improving controls and efficiency and effectiveness

of operations to achieve the organisational objectives (Gjerdrum and Peter 2011). Although there have been various designs and implementations of risk management frameworks and standards, there is no universal way of applying risk management processes without recognising their size, nature, and intended use. The participants elicit the contributions of risk management to ensure CSRM implementation success in their organisations.

In case study A, acknowledging that risk is a reality and the commitment to identify and manage risk is at the organisation's heart. All the participants stressed that risk management is important in CSRM. It is necessary to adopt one or more risk management standards/frameworks to follow for a successful CSRM implementation based on the organisation's context. The participants felt that risk management standards/framework form CS/information security risk management's bedrock. Hence, the CISO and Security Engineers who are experts in their fields treat the standards, for example, ISO 27001, as a 'Bible'. P3 added that:

> *ISO 27001 has been very effective at showing potential risks and loopholes in our setup and storing, sharing, and handling data. We are now equipped with the knowledge of best practices regarding CSRM.*

All the case organisations have adopted frameworks to suit the organisations' context and the necessary controls—Table 6.2.

Table 6.2: Comparison of Adopted Risk Management Framework by Organisation

Adopted Risk Management Standard/Framework	Case Study A	Case Study B	Case Study C	Case Study D
ISO 270001	✓	✓	✓	✓
ISO 37001	✓			
NIST	✓	✓		✓
CBN		✓	✓	✓
C2M2				✓
Business Continuity Standard				✓
PCI-DSS	✓	✓	✓	✓
COBIT5				✓

Table 6.2 clearly shows that none of the case studies adopts a single framework but combines the best frameworks to develop each organisation’s best practices for CSRM. This confirms no universal way to apply risk management, but the organisational context is critical (section 2.4.2).

The adopted Risk Management programme is based on understanding threats, vulnerabilities, risk profile and risk tolerance (CBN 2018). Suffice to point out that Case study D adopted most frameworks because the new CS framework prescribed for adoption as a guideline for all DMPs and PSBs derived from the combination of the best practices in most existing security frameworks. The comprehensive list is in the complete guideline (CBN 2018). P27 attest to this:

> *We had to draw from different standards to pick some points (P27).*

All the organisations adopt PCI-DSS and ISO 27001 standards, use payment cards and comply with the regulatory bank. Similarly, ISO 27001 is an Information Security Management standard, of which certification to the standard is mandatory. Case study A has its in-built framework built from ISO 27001, so most of the phases of ISO 27001 are represented.
P5 explains the process to design the framework below:

> *We examine the controls that serve the organisation's context better, have a demo around this to perform a holistic overview of all the systems, implement these controls, afterwards assess the adequacy of the controls to mitigate risk through monitoring.*

The key phases include risk assessment and mitigation phases. The risk assessment evaluates existing technical, operational, and management controls against assets, processes, and information threats.

All the participants asserted that adopting the standard is critical to CSRM implementation success. The CISO explained, in the E-retail, the risk management components, including risk identification, assessment, analysis, evaluation of impacts and mitigation plans, are around information assets and the classification of systems based on their functions, applications and processes. Any cyber/information security risk assessment focuses on critical areas of concern and prioritises its use of resources to maximise response and recovery efforts. The necessary risk management steps and guidelines by ISO 27001 and NIST are towards the controls.

In addition to the common frameworks adopted by all, case study B adopts the CBN framework but not ISO 37001. According to P11:

These standards help provide a framework to build our security program. They provide guidelines on the type of implemented controls that suit our business and reduce our attack surface.

The evaluation and management approaches to risk management evaluate the risks in past projects, identify the concrete events or situations within the projects that disrupt the plans, learn and develop measures to keep the project on track (de Bakker, Boonstra and Wortmann 2010). The outcome may often result in adjusting the methodology's use or even adjusting the methodology itself (de Bakker, Boonstra and Wortmann 2010). P14 asserts that:

A well-managed cyber risk program and environment do not add bureaucracy to the process; instead, it helps streamline and improve management processes and integrate corporate risk strategies. It defines operational policies, standardises procedures, and is more effective.

In this regard, a holistic approach to CSRM could distinguish failure and success. P14 extensively explain the choice and effectiveness of the adopted standards in the following comments:

THE holistic ISMS process is recommended to approach information asset risk management and CSRM by implementing an ISO 27001 standard and the CBN framework. They both cover the majority of the risk spectrum starting from CSRM Scope, Information security policy, Information security risk assessment and process documentation, Information security risk treatment, comprising statements of applicability, Information security risk treatment (Risk treatment process), Information security objectives and plans, competence, operational planning and control, Risk management procedures such as Risk assessment results, Risk treatment results, Metrics, internal security audits, CS management reviews/ ISMS, Nonconformities and corrective actions.

Case study C does not adopt NIST and ISO37001 but ISO 27001, PCI-DSS and CBN framework. The distinction is worth noting and highlights that CSRM can be understood and interpreted in many ways. Does this create a complicated landscape? The fact that organisations have acknowledged the need for risk management in the dynamic CS world is moving in the right direction. Thus, the Risk management sequence of activities defines the processes associated with

risk management to aid management decisions. In agreement with this notion, the gains of the adopted CSRM programme in the participants' words in case study C further explains that risk management as a success factor for CSRM implementation.

> *Implementing international and local standards and mitigating controls are taken from a few frameworks to suit the business needs (P22).*

> *Identifying, analysing, evaluating, treating, and monitoring the risk has been very useful as reviewed regularly for relevance (P18).*

In case study D, at the operations arm, P24 explains that the different risk management phases are divided into business functions to reduce cyber threats and attacks. For example, the security team checks/identify what the likely security issues that have to do with new implementation are? The quality and compliance team monitors the new implementation initiatives while the change and advisory board evaluate and approves. The regulatory arm encourages the financial institutions to certify global international standards, ensure and monitor compliance with the CSRM framework, and align and measure herself with the CS Capability Maturity Model.

Risk management's effectiveness depends more on people who set up, coordinate and contribute to risk management processes and less guiding framework. It is worth noting that people identify, analyse and act on CSRM factors and information towards implementation success, not frameworks. All the case studies participants affirm that they are fully certified and commend their implementation success to strict adherence to the standards. Most case studies employ qualitative risk analysis methods using probability and impact analysis as the tool and technique for risk analysis, while case study D uses SWOT analysis. The risk management method adopted by all proves effective because there is no record of any CS breaches, yet in the last five years. This awareness and rethinking of risk management processes posited by (Jean-Jules and Vicente 2020) confirm that these organisations have effectively used it to achieve CSRM implementation success.

- **Security Policies**

CSRM policies clarify the importance of CSRM to the organisation by defining the CSRM objectives and specifying the corresponding responsibilities of employees towards achieving the objectives (Ma, Johnston and Pearson 2008). Also, adopting a security policy is necessary as an

initial measure that must be in place to minimize the threat of unacceptable use and security of any organisation's resources/assets to ensure CS success.

The participants explained how CSRM policies have contributed to CSRM success in their organisations. Figure 6.11 below shows CSRM policies and sub-themes.

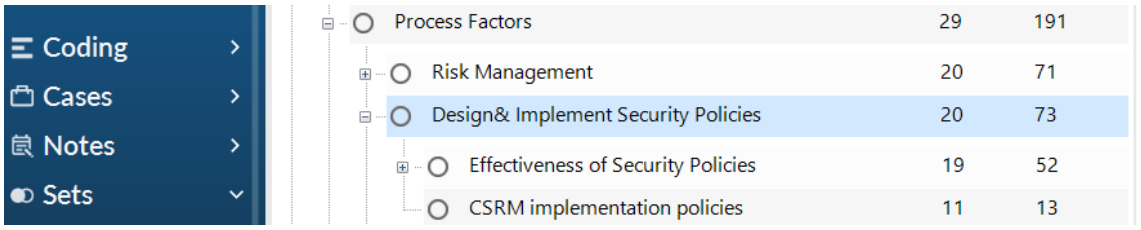

Figure 6.11: CSRM Policies Theme and Sub-Themes

The interviewees in the case studies discussed the security policies in their organisations and how effective they were in reducing breaches in the last five years.

Case study A has **recorded a high success rate** in implementing CSRM by enforcing **some security policies** for workflows and processes. CSRM policies include technical controls to ensure that processes, procedures, and workflows are strictly enforced, with or without proper supervision. P1 noted that despite continuously attempted breaches – none successfully penetrated yet. It is interesting to note and resonate that CSRM implementation success is at the heart of business processes in case study A. There is no room for none compliance but enforced with controls. Thus, the adaptation of the CS policy to organisational needs and objectives is necessary.

P12 from case study B comments:

> *P**olicies** and frameworks were developed to help the organisation prevent the foundations that would put the company to risk. The documented policies are shared with all staff to read and understand the processes and sign off. The framework is discussed at the top level; the senior management helped ensure the policy and framework are followed. So, the policies are still a plus in CS alignment with the organisation's objectives.*

Consistent with case study B, CS policies must align with the organisation's objectives and goals to achieve the desired result. P18 and P19 from Case study C established this:

> ***CSRM policies*** *and* ***controls*** *were designed based on several frameworks* ***to mirror the business's goals****.* ***These policies closely align with business objectives.*** *For instance, controls are in place to ensure customer data integrity that can dangerously affect the organisation's reputation (P19).*
>
> ***Policies have been relatively helpful****, but as technology advances, so do the sophistication of organisations' attacks; however, these policies remain effective—no CS breaches in the last five years (P18).*

Undoubtedly, policies serve as a framework that guides actions to what to do or ought not to do within the entire organisation. As a regulator, policies guide actions in case study D. Polices give a framework to systematically monitor and maintain key relationship management with the banks with zero tolerance for non-compliance. Thus, P24 concludes that:

> *CSRM implementation policies provide a framework to query any erring staff, thereby giving us a direction (P24).*

All the participants confirm that the enforcement of security policies aligned with the CSRM and that business goals and objectives necessitates awareness and training on security policies and implementation of technical controls, processes, and procedures. Compliance with security controls reduces breaches and the success of cyber-attacks. The respondent's acclaim that the policies are too many to mention but highlight the few relevant to CSRM success. Case studies A-D have similar policies such as email acceptable use policy, BYOD (Bring Your Own Device), Clear Screen Policy, Computer acceptable use policy, Network acceptable use policy, Multi-Factor Authentication (MFA) and much more. These policies and adopted CS frameworks create and automate the socio-technical aspect of device connectivity and adopt proper security controls and defences to minimise human vulnerabilities and systems risks enhancing CSRM success.

For the CS program to be successful, cybersecurity policy must align closely with the organisation's needs (Goss 2017). These analyses show consideration of some criteria for proper design, implementation of CS policies and successful organisational assets security. These are straightforward, non-technical, but easy to read and understand CS policies, state the purpose scope, and align with the organisational goals and objectives. These policies must be a living document that specifies all stakeholders' roles, responsibilities, and expectations to be effective and regularly revised to suit the organisation's needs. The findings are hardly distinguishable from

(Al-Awadi and Renaud 2007; Dawson 2018), who support that security policy is a success factor for CSRM.

- **Security Audit**

Further, to ensure CSRM implementation success, as discussed above, compliance with the CSRM policies and controls need to be monitored, evaluated and reported in a process known as a security audit. The participants rated the effectiveness of CS audit on CSRM implementation success. The participants unanimously agree that a security audit has been a critical factor for CSRM implementation success recorded in their organisations.

Case study A participant comments that the effectiveness of **CS audit** on CSRM implementation is **very high** since a CS audit's objective is to provide management with an assessment of an organisation's CS policies and procedures and their operating effectiveness. A security audit is critical in implementing the effectiveness of the controls, processes, and policies, without which there will not be a maker or checker. Therefore, monitoring continual improvement reports based on internal audits such as awareness and training effectiveness, process controls and data management designs and protections continually improves, leading to the record's overall success.

There are checks on specific implementation for those deployments to be a success. Consistent with case study A above, in case study B, according to P10:

> *The security audit helps to no small extent in CSRM implementation success with a score of 80/100.*

P6 succinctly substantiates previous findings:

> *The effectiveness of CS audits is high. A cybersecurity audit aims to ensure that: one, data security policies relating to the network, database and applications are in place- that is, the deployment of data loss prevention measures; Two, adequate network access controls implemented - Security controls are physically and logically established; and Three, Incident response programs are implemented. All these should be done during the CSRM implementation to be successful.*

An appreciable agreement is evident in Case study C, as experts stress the role of regular assessment, feedback, and recommendations by external and internal auditors in the effectiveness of CSRM implementation success. Information security auditors corroborate the stance that security audit is critical as it ensures the controls are efficient and sufficient to meet the requirements of CSRM and rate the effectiveness of CS audit as excellent.

Case study D lends support to previous findings from other case studies. The participants explained that:

> *The security audit has been very effective; it covers the technology and end-to-end processes (P30).*

> *The audit department is also interested in finding out whether those vulnerabilities have been mitigated and usually come around every time to check compliance and highlight the areas of weaknesses for remediation actions (P29).*

These assertions from the case studies concur with (Islam, Farah and Stafford 2018; Kahyaoglu and Caliyurt 2018) and confirm that security audit discovers gaps in the CSRM implementation process and checks organisational CSRM maturity levels. Thus, the security audit positively influences CSRM implementation's success and shows the interrelationship between the socio-technical factors. Figure 6.12 shows the effectiveness of a security audit in organisations.

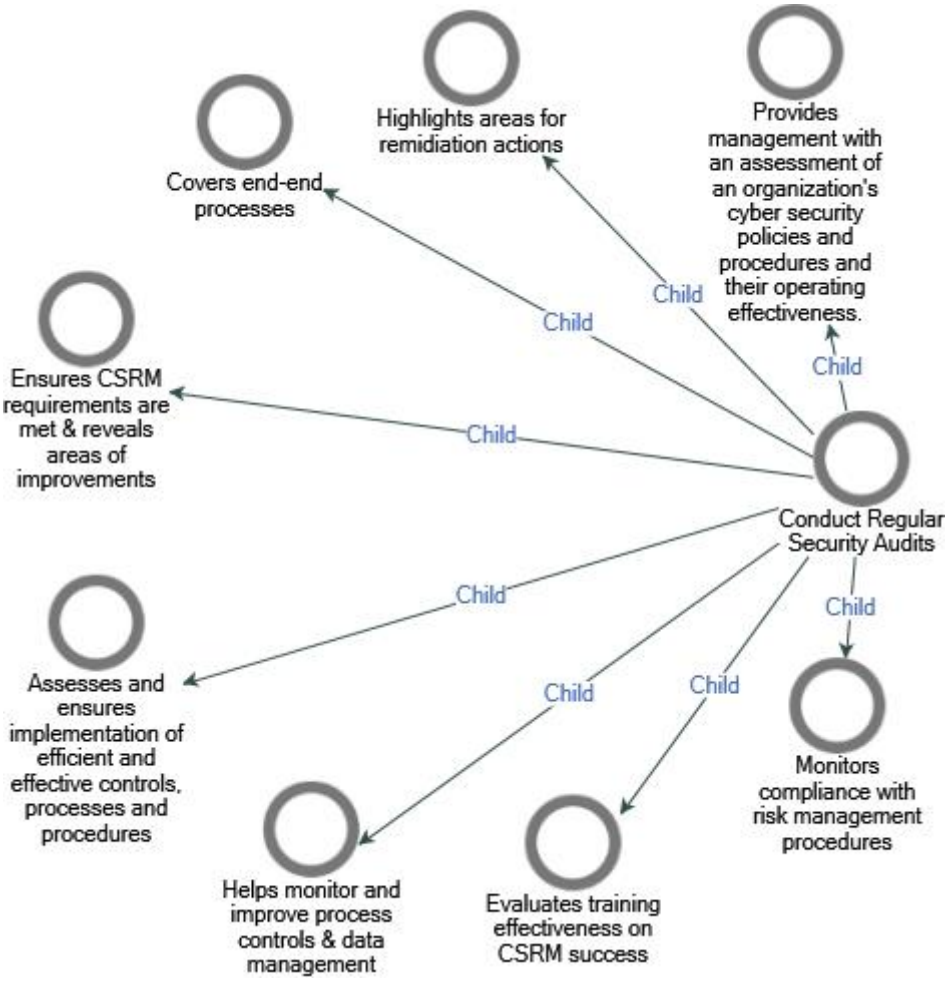

Figure 6.12: Effectiveness of Security Audit on CSRM Implementation Success.

In summary, while CSRM is becoming a business-related requirement, minimal spectacular, effective cybersecurity strategies and initiatives are most often successfully implemented in Nigeria (Okolo 2016; Oforji, Udensi and Ibegbu 2017. Processes consist of established techniques and comprehensive measures designed to achieve objectives. There is a need for organisational change factors that affect successful implementation.

6.2.4 Theme 4: Organisational Factors

The organisational factors focus on the CSRM strategy's alignment with the overarching organisational strategy and specific business needs and the governance structure. The organisation dimension answers research question 4.

What are the Organisational factors associated with CSRM implementation success in large organisations in Nigeria?

The theme and sub-themes are shown in figure 6.13 below and subsequently discussed.

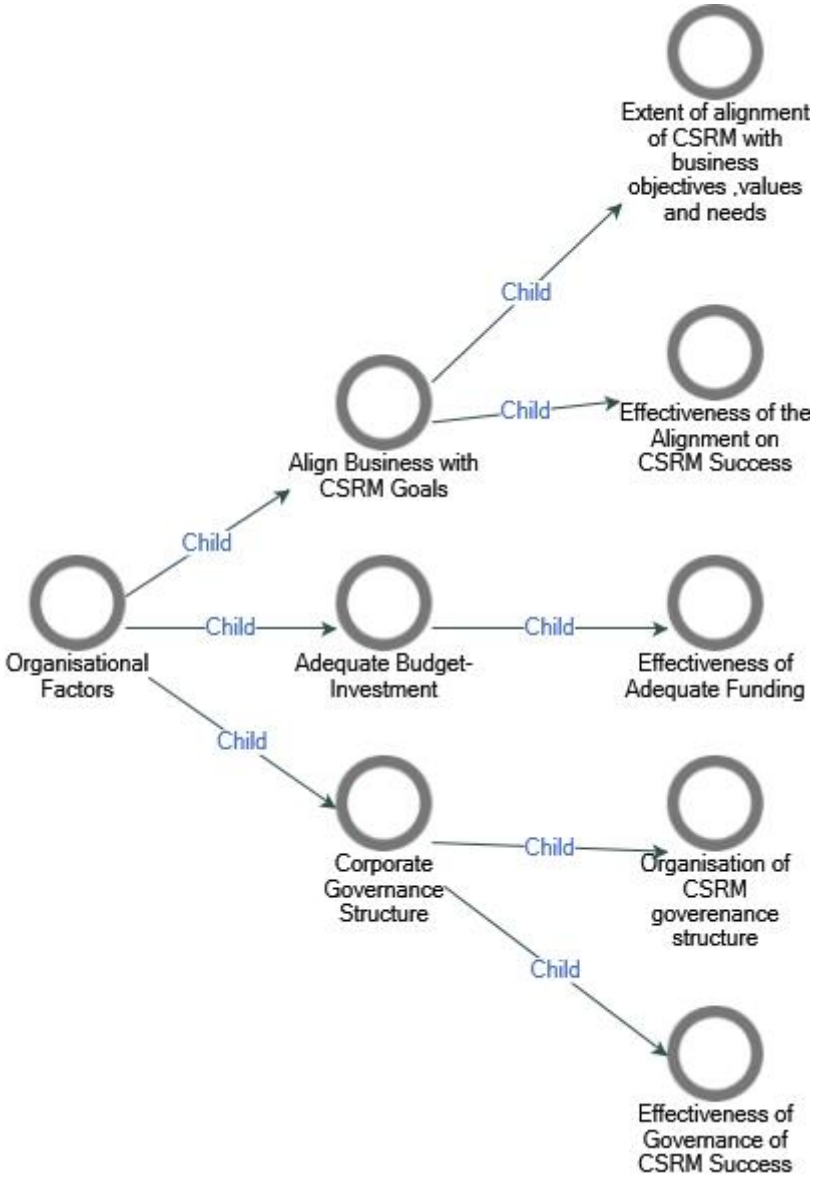

Figure 6.13: Organisation Factor Theme and Sub-Theme

- **Business Alignment with CSRM Goals**

In this study, the alignment of business activities and goals with CSRM goals means that risk management processes/tasks and goals fit well with other CS activities and business activities in the organisation. Alignment forms the bedrock for effective CSRM strategy execution (Srivastava 2017). A strategically focused or business-driven CSRM strategy is vital and should be aligned with the organisational objectives to be successful (Spears and Barki 2010; Tu et al. 2018).

Participants from Case studies A to D describe how their CSRM goals are well-aligned with the rest of the business objectives, values or needs. The interviewees' responses confirm that their business goals directly align with the CS goals. Case study A CSRM goals are directly dependent on the fundamental organisational goals. In setting the business objectives, the business processes are evaluated, and CSRM policies and procedures are developed to achieve the business objectives. Here are some of how business goals align with CSRM implementation to enhance CSRM implementation success. The CISO explained that:

CSRM implementation is designed to enhance business output, not just for security. First, define roles and responsibilities, capture the business process and develop policies and procedures in line with the business objective to enforce workflows and processes (P1).

The enterprise security manager explained that the CSRM implementation within the organisation involves technology, People, Processes and Policies. CSRM **Strategies align with other business goals** to **achieve maximum success**. Similarly, the risk manager believes that the CSRM objective cannot be separated from the organisational goals and objectives:

> ***CSRM objectives*** *must* ***align*** *with the organisational goals to be successful. Deviation from this is a recipe for failure.*

These findings confirm that the technical staff, the middle management and risk management staff perceived that CSRM goals are designed to align with business goals to achieve CSRM implementation success and not just for security's sake. It is fundamental to note that CSRM implementation does not operate in a vacuum but forms part of a business strategy. So, aligning it adequately with the business brings out the best outcomes and communicates the values clearly to stakeholders. Participants from case study B clearly acclaim that the CSRM implementation

broadly aligns with strategic business goals. P12 and P14 responses show how such alignment has created values:

> *A CS risk-managed environment's advantages include improved management processes and integration with corporate risk strategies and objectives (P14).*

By extension to the regulatory perspective and business processes, in the words of P12:

> *We have a **regulato**r that wants to see **alignment with Payment Card Industry Data Security Standard** (PCI-DSS) and ISO 27001 and always puts us in check. The aim is to secure clients' information so that we do not give our customers surprises in the future and our clients a reason to doubt us.*

Case study C goes on further on alignment from the management decision making perspective. Before making critical business decisions, the organisation adopts risk management standards and frameworks (ISO standard and CBN framework). In turn, CSRM policies and controls were designed due to the analysis and assessment of the frameworks to align with the business goals and objectives closely.

A security auditor explains that management and regulators recognise that using information technology to drive business also introduces CS risks, which is now an inherent risk in business cause CSRM implementation function to align with the rest of the business. The CSRM policies and controls were designed based on several frameworks to mirror the business's goals. For example:

> *The policies closely align with the business objectives; hence, controls ensure customer data integrity, which could affect the organisation's reputation.*

The information security committee responsible for the CS implementation programme's governance designed it such that CS, framework, and strategy align with the rest of the business. Similarly, CSRM goals align well with business objectives. P20 establishes this:

> *The risk management framework is considered when making critical business decisions and setting business objectives.*

In case study D, aligning CSRM strategies with the business goal is crucial. The organisation performs a dual role as a supervisor/regulator and an institution as a bank at the nation's heart. The organisation ensures that security and services align with the organisation's business needs using ITIL (Information Technology Infrastructure Library). The participants' comments:

> *Aligning CSRM to the business need is crucial to CSRM implementation success. We regularly review the CS programme and strategy to see where we are and align with the organisation's vision and mission (P23).*

> *We hand-picked mostly all the frameworks, so they are aligned to the business needs of the Bank. So, we have frameworks, guidelines, best practices to align the goals to ensure that we can compete with developed countries and everybody globally in best practices (P26).*

> *The CSRM team ensures that the CS strategies are relatable to C-level management by regularly explaining and communicating to the board how CS impacts business risk and business goals (P30).*

Furthermore, the interviewees highlight some effectiveness of aligning business goals with CSRM goals to ensure CRM implementation success. The analysis from Case study A shows a high-profit margin because the computer servers are safe from security threats and malware for customers' operational use. In case study B, CSRM's alignment with strategic business goals essentially **informed decisions** to **increase security focus on e-channels** such as ATMs and POS.

The organisation moves its customers to those e-channels. Case study C participants believed that CS risks' negative effect on business makes it paramount to evaluate and communicate this to the board. Evaluating the threats and risks to achieving the business goals leads to designing appropriate controls and mitigation practices for CSRM implementation success. Case study D elucidates the overall effectiveness of CSRM alignment with the business goals and concludes that a drastic reduction in information theft from servers in the last six months achieved a more than 70% success rate.

These affirmations support the literature that the business alignment with CSRM goals is a success factor for CSRM implementation. This alignment helps create a formal CSRM implementation

structure such that the managers at various levels of the organisation are more responsible and willing to support sound CSRM practices.

- **Corporate Governance**

This study defines corporate governance as the set of responsibilities and practices exercised by the Board and executive management to provide strategic direction, ensure the achievement of objectives, ascertain the cyber risks are managed appropriately and verify the responsible use of the organisational resources. Case studies participants explained how the corporate governance structure had influenced CSRM success in their organisations.

Case study A participants comment on a top-down model in which roles and responsibilities are assigned to support all strategic decisions for CSRM implementation success.
According to P1:

> *The organisation follows a **PDCA Model** where the **senior management remains the project owner. A top-down model is** in place to drive the principles of good governance, identify, assess, manage, and communicate risks elements to be treated using the PDCA framework to support risk-based decision making and oversight across all operations within the organisation.*

The expert team of dedicated CISO, Risk Manager, Security Engineers and the legal manager ensure the organisation achieves its business and security goals and objectives.

Some organisational postures may require a change in thinking or a change/implementation of business processes. Such may include specific roles of individuals toward CSRM could positively influence the effectiveness of CSRM strategy. Case study B carefully explained how corporate governance has helped CSRM succeed in their comments. Corporate governance is managed by three defence-operations/risk, control, and audit lines. A CISO led team manages cyber risk across the financial organisation. The CISO within the risk management directorate reports to the company Chief Risk Officer and periodic reporting responsibilities to the Board of Directors.
This governance structure shows the lead role that CISO performs in coordination, control management of CSRM operations and reporting to the Board as an audit function.

The suitable IT governance structures measure the success of CSRM or otherwise from time to time. Similarly, case study C participants confirm that there are three tactical and strategic levels of governance saddled with the governance structure of CSRM to enhance implementation success. The CISO, the IT security committee, compliance teams and a dedicated board-steering committee with oversite functions. P19 and P21 clarified the governance structure:

> *The tone at the top and board-level ownership has contributed a great deal to the success of CSRM (P21).*

> *The CISO reports to the CRO, who reports to the MD. Presentations to the information security steering committee on the business quarterly's security posture (P19).*

A governance body provides governance for CRSM initiatives and strategies. The CS strategy group meets regularly and reviews the CSRM implementation from key departments within the organisation's core business. In case study D, the CS strategy group of a key department oversees the CSRM success within the bank (the operative arm). In contrast, the supervisory arm ensures appropriate governance structures are in place in the supervised financial banks.
The CISO is an independent role, a governance structure, and a command structure from the regulatory perspective. The CISO, as much as possible, should be at least an Assistant General Manager.

Furthermore, the case studies interviewees commented on the corporate governance structure's effectiveness in ensuring CSRM implementation success. The majority responded in cases study A that the group governance structure has helped set appropriate plans and methodology for ensuring CSRM implementation success aligned with the organisations' standard policies.
Using a risk-based approach to improve CS governance, identifies and list company assets, develop a risk analysis management framework based on risk appetite, risk identification, risk impact, risk treatment, risk monitoring and continual improvements.
The data security analyst corroborated this statement:

> *We now have best-practice action plans, risk assessment and management, and compliance solutions focusing on cyber resilience/security, data protection, and business continuity with governance.*

Interestingly, as the topic is, case study B relates CSRM success with corporate governance by aligning CS with risk management function with defined roles and responsibilities for an efficient way of managing CS issues and risks. P10 and P11 stated that:

> *The governance structure provides clear responsibilities and ownership from the top (Board) (P10).*

> *This structure puts **CS as a risk management function,** which helps isolate it from the conundrum of battling for supremacy with technology leaders. Functioning as a risk management function gives CSRM the autonomy of tackling cyber risk issues wherever they exist within the business (P11).*

Also, in case study C, corporate governance provides direction for implementation for CSRM and the periodic report to the steering committee with appropriate feedback. This feedback assesses security postures, takes decisions to improve learning points and ensures strict compliance with processes, policies and procedures that ensures CSRM success. Also, recommendations from external audits perspectives help improve the governance function.

The corporate governance structure established by case study D ensures effective collaboration among deposit money banks, financial institutions, and payment system providers both within Nigeria and internationally. P26 explains that the inclusion of COBIT (Control Objectives for Information Technologies) as part of the organisation's integrated framework ensures a holistic approach to CSRM implementation success through security governance and organisational management needs. At least every month, the committee of CISOs meet and collaborate to share information on cyber-attacks or predictions on things that happen with other clients and modus operandi so that implementing those controls protects the organisation and systemic risk in the entire financial industry.

These statements and analyses from the case studies show that even though there are slight variances in the governance structures compared with each other, it is not particularly surprising that the position of the CISO is common to all. The concepts surrounding CSRM have prompted organisations to create a CISO post into an authoritarian stance on the organisational chart. In contrast to previous studies (Ashenden and Sasse 2013) and at the risk of offending some readers, there may be more possible explanations to the critical role CISOs have played in building better

relationships between the business and CS in realising CSRM success in these organisations (Dhillon and Backhouse 2001). Figure 6.14 depicts the effectiveness of corporate governance.

Figure 6.14: Effectiveness of Corporate Governance on CSRM Implementation Success

Figure 6.14 shows CS implementation as a risk management function (CSRM methodologies) with appropriate security corporate governance depicts the organisation as knowledgeable, unproblematic, and successful. The identification, assessment, management, and communication of risk elements to be treated through risk management led to risk-based decision making with clear ownership and responsibilities for risk management implementation success. These findings from the case studies agree with previous literature (Dhillon, Tejay and Hong 2007) that corporate governance, a critical component of CSRM implementation success, defines the structure, strategy, and methodology for CSRM implementation plans identify, assess, monitor, and mitigate organisational CS risks.

- **Adequate Budget Planning**

This study conceptualises adequate budget planning as having sufficient financial support to meet both the human capital resource needs and CSRM implementation activities and operations. Participants from case studies A, B, C and D explained how investment in CSRM creates value for the organisation. All the participants agree that the conviction and allocation of adequate budget to CSRM implementation goals and success had become the topmost priority for the management to avoid the substantial negative impact of any vulnerability in the system. The Data officer sums up in his response:

> *An investment in CSRM creates value in addressing risks such as asset protection, IT security, cyberterrorism, and crime. It also manages risk assessment and*

mitigation across the organisation, including the full range of security risks from asset protection to brand protection.

With much ecstasy, P1 commented:

It is hard to quantify the effect or impact of investments in CSRM and the value an organisation derives. How can someone rate reputational damage?

The usual trend of convincing the management is similar in case studies A and B before investing in CSRM. It is not unusual that case study B participants agree that it took long years to convince the management to invest in CS adequately. However, the participants' responses revealed that adequate budget planning created much value for the organisation in various ways.
P14 stated:

Making an upfront investment in a venture that does not bring returns is very difficult for organisations. As technology leaders, we present CS as an investment rather than a cost centre as a risk element. It took years for this communication to become effective, but once achieved, funding security investments became more comfortable even as it became evident that an increase in internet presence exposes the organisation to more risks.

Having secured management buy-in after success at creating awareness of CS risks and their damaging effect on the bank's reputation and considering the risk appetite (the level of risk they are willing to absorb to concentrate) and only focus investments on the significant risk exposures.
P12 added:

Investment in CSRM has helped keep our reputation and save money on issues that could have been costly to the company.

However, one of the participants ranked investment in CSRM implementation as fifty per cent because of the need for more improvement in adequate investment in CSRM.
Case study C participants are quick to comment on the overwhelming investment support for CSRM implementation in the organisation. They claimed that the management does not joke with CSRM implementation; primarily treat the IT department like a king, with much investment in human capital and IT resources. Therefore, key stakeholders are more confident when

approaching new and existing clients as a unique selling point. More importantly, corporate customers are willing to work with the organisation after reviewing the CSRM.
P16 explained that:

> *Investment in CRSM implementation has been very impactful and creating value for the organisation. High-end and top-notch CS solutions have reduced the number of CS incidents and e-fraud. For example, implementing dual authentication for some employees after one of the bank's fraud has helped reduce subsequent episodes, reduce the loss of funds, enhance investor confidence, more substantial brand equity and deepen customer trust.*

The participants in case study D also confirms that investment in CSRM is significant, and the management has invested much in CSRM implementation, making it easier to extract value. For example, P24 noted some key areas:

> *The organisation has invested significantly in CSRM implementation. A lot in technology, firewalls, monitoring devices, intelligence, staffing, staff awareness, monitoring devices to prevent an attack and ISO 27001 certification of key staff and the organisation.*

However, some participants believe the investment in CSRM might never be enough; the management can still do more.
The participants' effectiveness of adequate budget planning is shown in figure 6.15.

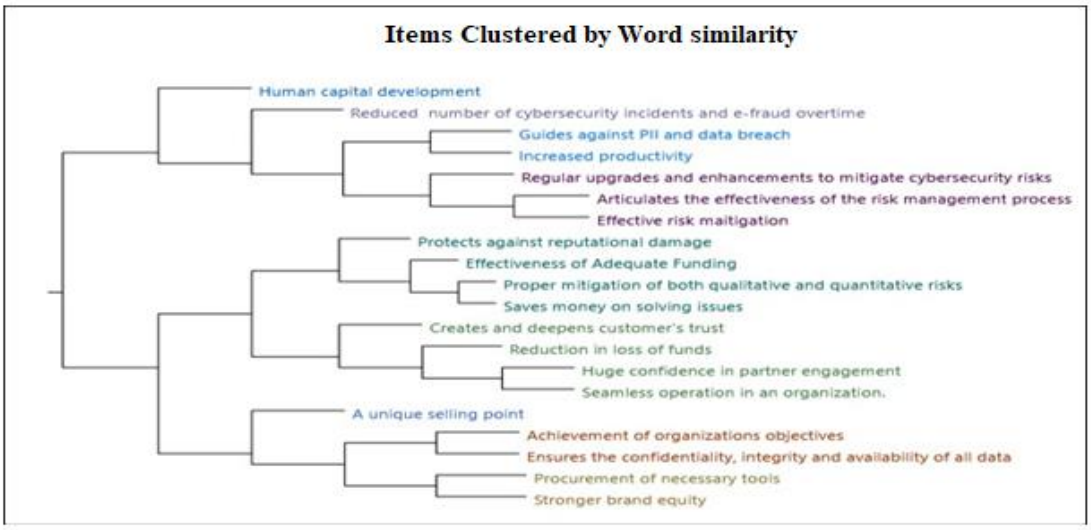

Figure 6.15: Effectiveness of Adequate Funding

Figure 6.15 demonstrates the relationship between the case studies' analyses suggesting that adequate investment planning is a success factor for CSRM (Tu et al. 2018). Investment in CSRM is directly proportional to the enterprise's value; more importantly, it prevents avoidable loss through CS events. Understanding the inter-relationships between the success factors is at the heart of the study. The cluster analysis of the word similarities of the themes provides an overview of the data structure. Cluster analysis based on similarities in qualitative data coding is usually more helpful for thought-provoking than explanatory evidence of association (Bazeley 2019). The correlation between the effectiveness of adequate funding is worth mentioning. Provision of adequate finance for regular upgrades and enhancements to mitigate CS risks ensures the CIA of all data. Proper mitigation of qualitative and quantitative risks saves money on solving issues; improved productivity leads to reduced CS issues and e-fraud related issues, leading to organisational objectives strengthening strong brand equity and reducing reputational damage. Therefore, there is a need for an optimal operational CS investment level for CSRM implementation success (Ekelund and Iskoujina 2019).

6.3 Framework Review

A recap of all the participants' factors within the interview discussions reviews the framework. The framework review by 23 participants in figure 6.16 is made of mixed feelings.

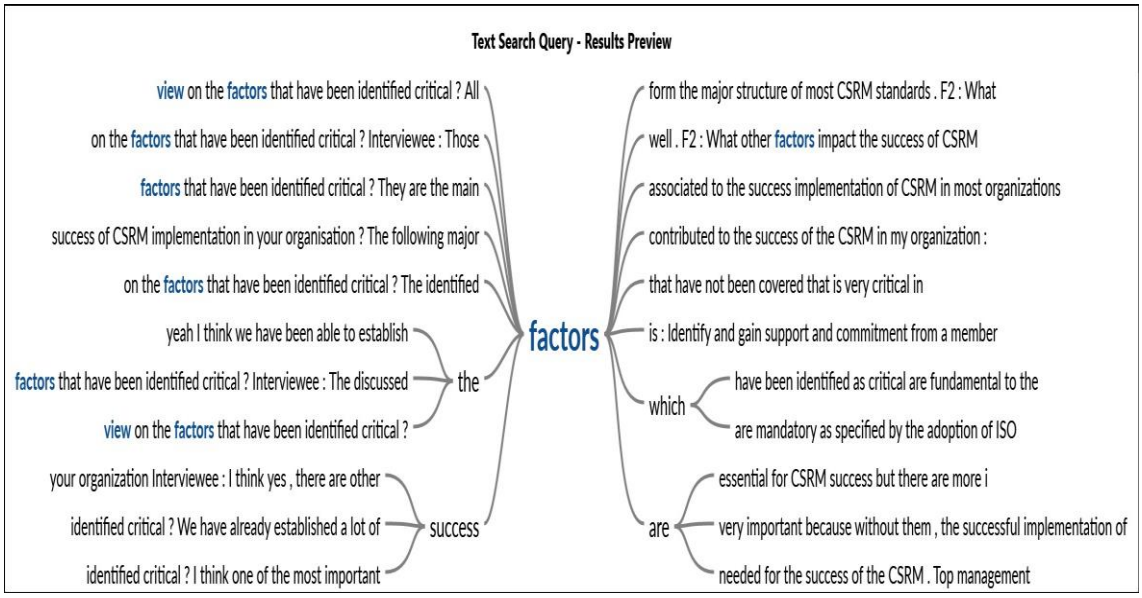

Figure 6.16: Overall View of Factors Identified

In figure 6.16, four out of the participants believed that although all the factors are necessary, more factors have not been identified and made further contributions. Nineteen considered that all the factors identified are 'germane', 'needed' and 'critical' and further embellished their importance. Two out of the 23 participants concluded the whole nine yards. That is, all the factors discussed are interwoven and equally important. Hence, a combination of all is necessary for CSRM implementation success.

6.4 New Success Factors from Case Studies

Although the framework gained merit primarily, some other success factors were suggested, as shown in figure 6.17.

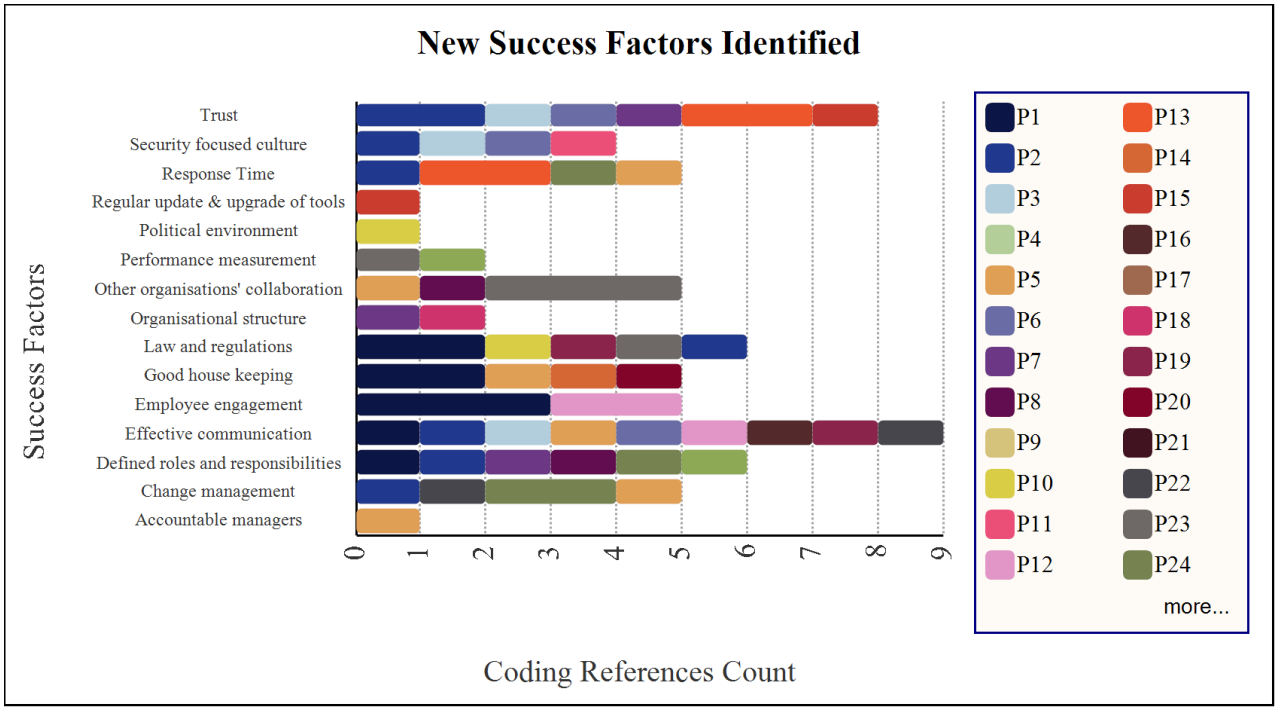

Figure 6.17: All-New Factors Identified

The case studies interviews identified twenty-four success factors. Although some of these factors were sparsely mentioned during the literature review, they were already discussed as part of the significant success factors themes and sub-themes. For example, the organisational factors theme is a management perspective that places CSRM within the organisational structure and corporate strategy (Kayworth and Whitten 2010; Tisdale 2016; Tu and Yuan 2014). Since multiple sources validated factors before being confirmed, the success factors that resonated among the interviewees were adopted, discussed, or highlighted in the literature review. Those with no direct effect on CSRM implementation success were discarded in line with (Petter, DeLone and McLean 2013). They are discussed below:

Organisational Structure: Although corporate governance was a higher form of organisational structure, the organisational accountability structure that constitutes the social dimension that enables systems of authority, communication, and work flow (Masike, Sune Von and Marnewick 2019). The organisational structure aims to emphasise functions executed by a particular process or competency to attain CS implementation (Masike, Sune Von and Marnewick 2019). Two participants comment that organisational structure is considered a significant factor contributing to the success of CSRM in the organisation. For example, P7 stated:

The organisational structure provided the concept, guideline, direction, and support to the employees and how to apply CSRM to the various business units.

In agreement with previous literature, the organisation structure is an essential success factor in information security implementation in Malaysian public service organisations (Dzazali and Zolait 2012) and other earlier studies as a form of coordination mechanism comprising roles and responsibilities, communication, values, cultures, and reporting structures (Kayworth and Whitten 2010; Tu et al. 2018). Organisation structure affects the task, the people, the project, and the IS (Petter, DeLone and McLean 2013).

Security-Focused Organisational Culture: A study of an effective CSRM implementation success would be incomplete without a focused, conducive, and encouraging CSRM organisational-wide culture. A CSRM focused organisation positively impacts social and technical factors to achieve the necessary support for CSRM implementation success. Four participants commented that the organisation's security culture had been a factor that controls the organisations' decisions, activities, acceptable behaviours, and processes. A participant noted that it is common to make slowly and quickly downturn decisions and management styles in Nigerian culture. Therefore, P2 and P11 supported that a security-focused organisational culture is influential:

__Organisational Culture__ is another success factor. As an organisation, we have built a __culture focused on security__ when using an organisational resource (P2).

Staff and users have __security-focused culture__ embedded in everyday work (P11).

In summary, CSRM culture characterises the DNA that runs within an organisation regarding the value and pursuit of CSRM of all organisational assets, especially the CIA of the information assets.

Change Management: Change management involves the process, techniques, and tools to manage people and change to achieve the business outcome. Organisations operate in a dynamic environment where threats and technology necessitate a high change rate to keep up with the CS domain dynamics. Four participants identify change management as a success factor for CSRM implementation. For example, P30 comments:

CSRM is an agile environment where there is little time for threat modelling. This is a risk to the business that must be managed swiftly and effectively.

Organisations respond to these challenges by developing teams and processes, which can quickly rise to these challenges. Therefore, certain operations serve as guidelines for most activities (Change Management Process) by the change advisory board. P24 explains:

The change advisory board must evaluate the security team's need for implementation before approving deployment in the work or security environment.

This is necessary to ensure the successful implementation of any CSRM implementation countermeasure because it is essential to be aware of the implications of changes and manage such changes formally.

Effective Communication: Nine participants identified effective communication as a critical success factor for CSRM implementation. Communication is a way of information dissemination that must be clear and convincing for every stakeholder to understand. CSRM policies, procedures, processes, training, and awareness programmes must be well communicated to the stakeholders to educate staff about the organisation's risks and actions taken to mitigate them. Case study A participants stressed that communication is one of the factors adopted to implement CSRM successfully. For example, P1 and P2 stated that:

One of the beauties of communication as a critical success factor is sensitising employees to share nuggets like a cartoon-like animation for awareness about CS animating what they should do or not do (P2).

Policies, procedures, or countermeasure training programmes form part of the company living documents. These documents undergo quarterly review and updates communicated appropriately and what they expect to achieve (P1).

Defined Roles and Responsibilities: Six participants agreed that roles and responsibilities are a success factor for CSRM implementation success. This is important because for any organisation to succeed in any implementation programme, there must be a clearly defined role and responsibility assigned to a particular team. This ensures that the organisation and staff follow best practices through the accountability of the departmental heads and dedicated project

implementation, team members. Stakeholders must be informed of their roles in ensuring CSRM implementation success. P1 explained that the first approach in CSRM implementation success is to define roles and responsibilities. Most participants explained that the organisations are role-based systems, and security teams/committees are vested in ensuring compliance. The words of the P2 and P8 buttress this assertion:

> *A saying goes that a goat owned by the whole village will die of hunger (P8).*

> *There is a team tasked with ensuring the organisation follows best practices. This team includes the CISO, Security Engineers, Risk Manager, and legal manager. The CISO and Security Engineers are experts in their fields and treat the standards, for example, ISO 27001, as a 'Bible' (P2).*

The above affirmations agree with the literature that clear security roles and responsibilities and requisite knowledge of risk tolerances through policies, awareness and training sessions are the catalysts to implement acceptable preventive and mitigation CSRM implementation responses (Trim and Lee 2014).

Laws and Regulations: Section 3.3.2 established that organisations are social-technical systems vulnerable to the influence of their surrounding external environment (Chen and Mykletun 2014; Davis et al. 2014). Laws and regulations, political environment and geographical locations represent environmental factors that influence the organisation's social and technological parts from achieving its CS and organisational goals (Davis et al. 2014; Wu et al. 2015). These environmental factors can influence and impact both the organisation's social and technical security attributes. Therefore, the environmental factors span social and technological dimensions (Masike, Sune Von and Marnewick 2019; Yasin, Czuchry and Small 2018).

The participants decry that there are no laws specific for CS in Nigeria; although there are few regulations, the legal system is often an issue. P14 and P23 believe:

> ***Laws and Regulations*** *are critical factors to CSRM implementation. People are now more into various forms of obnoxious cyber activities such as cyber fraud ……., but the laws are not there for CS (P23)*

> *The legislative tools or compliance regulations/frameworks regarding CSRM implementation in Nigeria are another way forward (Nigeria's Official National CS Policy and National CS Strategy) (P14).*

In agreement with McCurdy (2020), some participants explained that the Cyber Security Act, which was passed into law in 2015, is not perfect, and the enforcement agents need the training to understand what CS is. This crunch legislation is adjudged more symbolic and peripheral than practical. However, legislative tools or compliance regulations/frameworks for banks and financial organisations are mandatory (Nwankwo and Ukaoha 2019). The participants explained that these frameworks and legislative requirements for implementation and continuous monitoring had enhanced CSRM implementation success in their organisations to a great extent.

Political Environment: As explained above, the political environment could have varying influences and impacts on an organisation's social and technical CSRM attributes. Organisations do not operate in a vacuum or silos. Most developing nations operate in a complex and turbulent environment that poses external risks and necessitates strategic Business-IT-Environmental alignment to achieve CSRM implementation goals and objectives (Pavlou and El Sawy 2006: Yayla and Hu 2012). The participants further explained that Nigeria's feeble government policies and regulations make organisations concentrate more on CSRM implementation success efforts. P10 suggested the political environment as a success factor for CSRM implementation with comments:

> *The political environment is a success factor as well as a failure factor. CSRM implementation success has to do with regulations and government providing enabling environment for organisations to share information in CS breaches, learning points and prosecuting cybercriminals. When there are no laws and regulations against cybercrime, how does an attacked organisation get justice/compensation?*

Cyber security policy combines methodologies, techniques, laws, and regulations to protect organisations from security threats (Al-Awadi and Renaud 2007). Laws and regulations and political environment align with some literature proffering solutions to CS challenges in Nigeria (Osho and Onoja 2015; Saulawa and Abubakar 2014). In a significant advance study on CS legislation, Ogu, Ogu and Oluoha (2020) propose a feasible and operational globally adopted and unified global CS legislative framework presently lacking worldwide. To this end, this study

hopes that the recent national cybersecurity policy and strategy (2021) will be focused and alive to enhance CSRM implementation success in Nigeria.

Response Time: Time is a central variable that respects the very idea of dynamics of the CSRM implementation process identified by four interviewees. Organisations need to commit proactively and genuinely to taking all possible steps and measures to identify CS risks, immediately respond and resilience peradventure an attack or breach is a distinguishing factor in CSRM implementation success.

One key project success measures in any project management is that a project must finish on 'Time', 'budget' and 'quality'(Bannerman 2008; Camilleri 2016). Likewise, the triplet is famous for CSRM implementation success. Time plays a significant role in deciding the failure or success of CSRM implementation projects. For example, the participants explained that an all-around response time must address issues. For instance, timely and systematic human capacity development and vulnerabilities management is essential, especially in up-to-date patches.

Trust: Despite the increasing development in e-commerce and the adoption of e-banking services in Nigeria, some customers still are reluctant to consider e-banking services due to lack of trust and associated risks with internet services (Hu et al. 2020); Usman and Shah 2013). Organisations strive to build trust in customers by using their web services to sustain a good reputation and business profits by ensuring that CSRM implementation is successful. P7 and P13 buttress Trust as a success factor in the following words:

> *Trust is also a critical factor. CSRM is a form of insurance for an organisation that does business online. The first point of call in any business to implement an excellent CSRM procedure concerning customers is* ***trust*** *(P13).*

> *Trust, they argue, enhances working relationships, solidifies partnering roles and increases the willingness of various project stakeholders to cooperate. This comes from sharing materials, information, resources and displaying good intent behaviour from the staff (P7).*

Organisations Collaboration: As discussed in section 4.20, collaboration amongst other industries, both local and international, enforcement agents and regulators must be current on the latest developments in the CS domain and share experiences while learning from one

another. For example, unfailing security monitoring and incident response, resilience, disaster recovery and the development of forensics (digital evidence) in CS incidents.

> ***Collaboration i****s essential in CSRM. We also collaborate amongst ourselves, and the financial institutions rely so much on collaboration (P23).*
> *Another factor that impact the success of CSRM is* ***collaboration*** *with other organisations within the industry (P8).*

Also, from the pilot interview, one of the participants expressed collaborations as a success factor for CSRM implementation. Contrary to expectations, a further probe of the practicalities and additional insights into how organisational collaborations has helped revealed no external collaboration with other organisations on CS best practices or breaches from case studies A and B. P1 and P10 are united in their views and sadly expressed that:

> *Collaboration with other industry or government agencies is exemplary. However, it is practically non-existence now. We have not seen much collaboration on CSRM among organisations. However, we see an element of collaboration among regulated industries like the banking sector (P1).*

> *Although collaboration is crucial, there is none (P10).*

Nevertheless, collaborations exist within the organisational departments and third-party suppliers, such as insurance and cloud security. This is so because there are still no better laws and skilled law enforcement personnel in the country.

Performance Measurement: Performance measurements have been discussed in section 3.4 as the organisation's security implementation measures. The participants believe that performance measures drive stakeholders and the entire organisation towards CSRM implementation success and achieve organisational goals. A participant commented:

> *If the banks know that they will receive a penalty if they do not comply with regulations and laws, CS compliance is 99.99%. This has led to CSRM implementation success (P25).*

Nevertheless, all organisations have no suitable performance measures (Skibniewski and Ghosh 2009).

Employee Engagement: Engaged employees offer support, own, and control the CSRM implementation process. Employee engagement was suggested as a success factor for CSRM implementation by the CISO in case study A. Here are the comments:

> *Organisations are majorly dealing with weaponised codes broadcasted across the internet with the ability to mutate and self-replicate. For CSRM to be successful, employee engagement is one must-approach from a multidimensional perspective.*

Another interviewee suggests employee engagement factor as the user's cooperation in Case study B and comments:

> *User cooperation is a critical factor because no matter how intense the policies are or how good the technology state is, non-supportive system users will form a weak link. If there is a weak link, the whole process is just a mess, so I think user corporation is key (P12).*

Although there were references to the role of employees in CSRM, particularly in awareness and training programmes and policies, Albert Einstein in Mitnick and Simon (2011) states that:

> *Only two things are infinite, the universe and human stupidity; I am not sure about the former.*

That is, CS success can occur when humans are not ignorant about acceptable security practices. Engaged employees revise and recreate understanding and interact purposefully for the benefit of all stakeholders. In agreement with the literature, employee engagement mitigates user negligence and employee compliance. Security policies and decision making (Chabinsky 2014) through interaction at risk workshops enhance a risk-free cyber organisation (Mikes and Kaplan 2014; Siponen, Mahmood and Pahnila 2014). Likewise, the engagement of subject matter experts with requisite skills and expertise assisted in the design, development and deployment of necessary security controls and training, among others that influence CSRM implementation success.

Cyber Hygiene: The CISO in case study A suggested cyber hygiene as a critical success factor in CSRM implementation. According to him, the most impactful cyber breaches in the last ten years occur because of negligence in doing the simple but basic adequate controls of CS. Examples are password policies (i.e., having a password and regular password change), inadequate training of users, and all other security protocols. He further clarified that cyber hygiene is synonymous with good housekeeping. Hence, organisations must implement a standard risk management framework to systematically address the underlining housekeeping checklists integrated within the managed standards or framework. This further confirms the need to balance practice and processes to the letter no matter how small based on the implemented framework with good organisational and people behavioural factors.

> *The most effective deterrent to cyber risk is good cyber hygiene; good cyber hygiene is critical in CSRM implementation success.*

The above explanations highlight the interwoven role of cyber hygiene as a human-business issue across this study's four major themes- people, process, technology, and organisational contexts in ensuring CSRM implementation success. However, 'good housekeeping is one of CS's necessary routine activity/checks (Trim and Lee 2014:163). A further study on cyber hygiene in literature in CS contexts revealed two common themes from individual and organisational contexts (Maennel, Mäses and Maennel 2018). Cyber hygiene from human behaviour relates to adaptive knowledge and behaviour regarding CS risks; the organisational context relates to the business and applying standards (set of practices) concerning technology and implementing the CSRM framework (Neigel et al. 2020; Vishwanath et al. 2020).

Although, there was no evidence to support its importance on CSRM implementation success across the case studies partly because cyber hygiene is subjective, depending on the organisational context (i.e., organisations will implement cyber hygiene differently). However, this study chose to focus on factors that directly affect CSRM implementation success. Sub-themes and activities classified as control factors/elements of each factor discussed by the interviewees are included in the model development, such as cyber hygiene (simple practices, but ultimate sophistication), top management leadership and commitment and many more considered critical to CSRM implementation success. They are, therefore, classified as a controlling factor.

6.5 Chapter Summary

The chapter addressed those factors considered influential for the successful implementation of CSRM in large organisations in Nigeria. The chapter employs supporting themes as guidelines broadly classified as Organisational, People, Process and Technology factors. The resulting themes provide sufficient insight to identify and evaluate a success factor. Each case organisation identified and evaluated the same factors with mixed feelings by ascribing more importance to some factors influencing CSRM implementation success.

This chapter helped address the research objectives by identifying and evaluating success factors influencing CSRM implementation in large organisations in Nigeria by the experts in practice. The chapter also collates the findings from the various research phases and compares and critiques the literature findings. The triangulated research process culminated in evaluating and improving the success factors and the research phase. The success factors were identified and discussed alongside the associated sub-factors and activities. The case studies assisted in the in-depth understanding and evaluation of the success factors and obtained valuable insights from the interviewees.

The findings of this study reflect a total of 24 identified success factors. Because these factors were identified, evaluated, and verified in practice by industry experts, the first-hand experience in implementing the CSRM added more credibility to the results. It also provides the foundation for developing and refining the conceptual CSRM implementation model discussed in the next chapter. The overall findings of the research and the revised model are discussed in the next chapter.

Chapter 7: Revised Framework

7.1 Introduction

The preceding chapter examined the research questions stated in Chapter 3. The socio-technical theory was extended and applied to identify the success factors for CSRM implementation, particularly in Nigeria. This was to produce a helpful output as a guideline to both researchers and professionals in practice. The adopted triangulated strategy achieves this, and the combination of data sources enhances the validity of interpretations and academic rigour to this study. The analytical method minimises the drawbacks of using a single source.

Chapter 6 presents the comparative analyses and discussions of these case studies conducted in four large organisations in Nigeria. Qualitative findings shed light on essential aspects and identify various factors. In some cases, there are agreements, and in others, there are disputes. Moreover, in several instances, the findings reflect the currently existing literature. The empirical evidence and findings from the comparative analysis indicate the need to modify the conceptual model, as proposed in Figure 3.1. The current chapter considers the empirical data to revise the conceptual model based on these findings and present a synthesised success factor model for CSRM implementation. As a result, satisfy the aim and objectives of this thesis by proposing to the decision-makers and researchers a model of success factors for CSRM implementation in large organisations in Nigeria.

7.2 Integrating Findings and Learned Lessons from the Case Organisations

This thesis offers a broader understanding of success factors influencing CSRM implementation in large Nigerian organisations. Success factors for CSRM implementation were explored and interpreted with a unified viewpoint filtered from related CSRM implementation research and practice. The approach's values are scarcely distinguishable (Jean-Jules and Vicente 2020; Marble 2000; Orlikowski and Baroudi 1991). Therefore, the lessons learnt result from the explanations provided and are not prescriptive but further used as guides for CSRM implementation puzzles, decisions, and actions. These lessons might be helpful to large organisations in Nigeria as well as IT practitioners, implementers, risk managers and researchers and are summarised below:

- **Lesson 1**: Awareness and training programs could be likened to a sales marketing outreach. Employees should understand CSRM implementation success's values rather than strict policies and penalties as punishments.
- **Lesson 2**: Allowing employees to realise their full potential by being creative in CSRM awareness and training programs through employee engagement allows for novel discoveries and more productive ways to enshrine the CSRM culture in the employees that resonate well over a long time.
- **Lesson 3**: CSRM implementation success occurs when people are not ignorant about acceptable security practices by constant reminder and consciousness through awareness and training programs. Knowing the latest security trends through webinars, collaborations with other groups within and outside the industry are vital. Else, CSRM implementation success becomes a mere illusion or wishful thinking.
- **Lesson 4**: A more distinctive way to ensure CSRM implementation success is to adopt appropriate risk-based governance concepts and structures. Management should build trust in employees to be active participants in CSRM implementation success and not perceived as weaker links. Through collaboration, the stakeholders work in one direction to build a resilient CSRM culture.
- **Lesson 5**: The CS issues today is not about blaming users for falling prey to social engineering but stopping the issue from happening by bringing the right team together with competent IT skills and knowledge, gaining management support, availability of resources and ensuring that there is a joint optimisation (a balance) between prevention, detection, and response within a CSRM based implementation framework to mitigate CS risks and threats.
- **Lesson 6**: Cyber hygiene ensures that the simple but effective controls, no matter how small based on the framework implemented, are not missed or ignored.
- **Lesson 7**: The socio-technical approach to identifying and evaluating CSRM implementation success can reveal and address the latent and emergent risks that might result from the complexity of current and proposed CSRM implementation practices focusing on new technologies.
- **Lesson 8**: The meaningful extension of methodological analysis to address the enormous problems of global concern in practice environment may suggest the reaching limit of the traditional tendency to explore success factors in security research. Models that inspire scientific approaches have limited ability to address emergent properties of such organisations and the CS domain.

- **Lesson 9**: CSRM implementation success is a continuous and dynamic process that impacts the entire organisation. Therefore, it requires excellent and adaptable change management plans and implementation embraced by all.

7.3 The Revised Success Factors Model For CSRM Implementation in Large Organisations in Nigeria

Having completed the empirical findings, as described in Chapter 6, promises are often not kept because of the emergence of the interpretive turn, reasoning tools. Qualitative research that uses interpretive and theoretical framework further shape this study (Creswell 2018).

7.3.1 Findings and Revised Success Factors for CSRM Implementation

It is proper to review and amend the proposed conceptual model (Figure 3.1) about the findings in Table 7.1.

Table 7.1: Analysis of Existing and Revised Success Factors for CSRM Implementation in Case Organisations

	Factors	Case Study A	Case Study B	Case Study C	Case Study D
People	Top Management Support	Top management support is very critical for the success of CSRM implementation	Top management support is very critical	Top management support is significant and key.	Top management support is required to ensure the longevity and success of the programme.
	Awareness	Awareness education is so important in CSRM implementation.	It has contributed to some extent in a big way.	CSRM deficiency has reduced by a big deal through awareness programmes.	No matter the technical effort, if people, or the workforce, are not aware, CSRM implementation success is unachievable.
	Training	My organization depends on training as an inevitable factor for CSRM implementation success	Training has reduced CSRM deficiencies as users better understand the risks inherent in their activities and ensure adherence to the recommended controls.	The risks to the business have been reduced through awareness training	Training is important for our organisation from the board to the users. An aware staff possess less risk to the organisation.
	Organisational Collaborations	Collaboration is essential but not seen much with CSRM among organisations.	Collaboration with other organisations within the industry is crucial but not in existence.	We work with our partners as much as possible, so those are our holistic risk-based approach to CSRM implementation success as an organisation.	Financial institutions rely so much on collaboration; we collaborate among ourselves within Nigeria and internationally.
	Trust	Trust is also a critical factor.	CS is a form of insurance for an organisation that does business online. Trust should be the first point of call for both customers and staff to implement an excellent CSRM procedure and practice.	Customers trust and satisfaction in our CSRM serve as a unique selling point for our organisation	The whole essence of CS revolves around customers trust in their data security in financial institutions. Trust is a great driving

					force in CSRM implementation.
	Employee Engagement	For CSRM to be successful, employee engagement is one must-approach from a multidimensional perspective.	User's cooperation is a critical success factor.	Not specifically mentioned.	Not specifically mentioned.
Organisation	Business Alignment	CSRM objectives must align with the organisational objectives to be successful. Deviation from this is a recipe for failure.	CS does not operate in a vacuum. It is part of a business, so aligning it adequately with the business brings out the best outcomes and makes all stakeholders see the values clearly.	CSRM goals must align with the business goals; else, the organisation will not function effectively. There will be cases of security issues. Both must work together.	Mostly all the frameworks align with the business needs of the Bank because they are hand-picked. So, we have frameworks, guidelines and best practices to align the goals.
	Corporate Governance	With corporate governance, we now have best-practice action plans, risk assessment and management, compliance solutions with a particular focus on cyber resilience/security, data protection and business continuity.	This governance structure puts CS as a risk management function which gives CSRM plenty of autonomy to tackling cyber risk issues wherever they exist within the business.	Governance has provided the direction for CSRM implementation.	Our CS governance contains a set of management tools, a comprehensive risk management approach and an organization-wide security awareness program.
	Investment/Budget	Investment in CS has become the topmost priority.	Funding security investments became more comfortable to achieve even as it became apparent that the organisation was exposed to more risks as it increased internet presence.	Funding has been very vital in the success of CSRM in my company.	Top management support and adequate funding are key to CSRM implementation success.
	Roles and Responsibilities	There is a team tasked with the responsibility of ensuring the organization follows the best CSRM practice. The first	Assignment of roles and responsibilities is an excellent factor in CSRM. A saying goes that a goat owned by the whole village will die of hunger.	The CSRM implementation strategic team ensures everyone performs his role in	The organisation is more of a role-based organisation. So, the organisation divides the function into

		approach is to define roles and responsibilities.		aligning business needs with the security needs	different units. So, monitoring and implementation are different in our office.
	Security Culture	We have adopted some factors such as commitment and support from top management, communication, organisational culture, trust and training to aid in the successful CSRM implementation.	The objective of our awareness training is to create a cyber-risk-based culture.	The bank is continuously improving security culture to drive embeddedness of security into daily transactions.	We invest in training a lot to ensure we build a security culture in each employee
	Effective Communication	I think communication has been a success factor.	The truth is that CS cannot thrive if there is no effective communication.	Communication of the process to stakeholders and what it intends to achieve.	We have multi-modal means of communication about CSRM. Communication is key in all areas of the implementation programme.
	Organisational Structure	An organisational structure is one of the significant factors that contributed to the success of the CSRM in the organisation.	Not validated	The CSRM governance structure is embedded in the overall organisational structure for effectiveness	Not validated
Process	Risk Management	The CISO and Security Engineers are experts in their fields and treat the standards, for example, ISO 27001, as a 'Bible'.	A well-managed cyber risk program does not add bureaucracy to the process. Instead, it helps, in most cases, to streamline the process and more effective.	Implementation of both international and local standards have helped us in our CSRM implementation success.	We adopt the CSRM framework released by CBN and ISO 27001 information security management standard to manage CSRM implementation success.
	CSRM Policies	So far, we have recorded a high success rate because of	About 80/100 success rate.	The CSRM policies and controls were designed based on several	The overall policy is one; there is zero tolerance to non-compliance.

		the enforcement of some security policies.		frameworks to mirror the goals of the business. The policies closely align with the business objectives.	
	Change Management	The change management process in place from most operations, and they more like serve as guidelines for most CSRM activities.	Not validated.	Not validated.	The change management board evaluates, assuming we want to have the implementation of a new initiative.
	Response Time	Rapid response time whenever a request comes in, even in the middle of the night, someone picks it up and starts.	Yes, other success factors have not been covered that is very critical in our organization but one. I would say response time.	Not validated.	At our implementation department, the questions to us are patches up to date? Have the vulnerabilities been mitigated?
	Performance Management	One of our CSRM implementation success measures is how many breaches we currently encounter compared to the time before the CSRM implementation.	There is an audit department responsible for regular monitoring of implementation success. Performance measurement is a success factor on its own.	We defined several metrics during the implementation of ISO 27001 and the CBN CS framework.	We also have some key success factors that we have prescribed to ourselves as part of our performance measurement.
	Security Audit	A security audit is critical in implementing the effectiveness of the controls, processes, and policies.	CS audit helps to no small extent in CSRM implementation success with a score of 80/100.	CS audit is critical as it ensures the controls are efficient and practical to meet the requirements of the CSRM.	Very effective. The audit not only covers the technology but also covers the end-to-end processes.
	Cyber Hygiene	Cyber hygiene is a critical success factor for CSRM	The most effective deterrent to cyber-risk is good housekeeping /cyber hygiene.	Not mentioned.	Not mentioned.

Technology	IT Competence	The IT team comprises subject matter expert skillsets.	The factor is considered at recruitment phases- the ability of the staff to have above-average ability to work with technology.	Individuals with a good understanding of the requirements of CSRM are in place to help ensure its success.	We have dedicated and committed staff in our CS programme. It is not everybody that we have; we have passionate people.
	System Quality	Technical control is a significant part of CSRM implementation. The quality of our technology systems is paramount.	We use monitoring tools to detect, prevent & sanctions for violations; they will not comply without these.	These technology solutions have had a tremendous impact in protecting these assets as they enforce the controls even when users do not.	We leverage technology, state of the art technology, especially new technology like Artificial Intelligence and machine learning to help us in our CS programme.
Environmental	Political Environment	Not mentioned.	I think Political Environment is a success factor for CSRM implementation.	Not mentioned.	Not mentioned.
	Laws & Regulations	Legislative and regulatory considerations may be applied to the treatment of the identified unacceptable risks.	The legislative tools or compliance regulations/frameworks with regards to CSRM in Nigeria is another way forward.	The regulatory requirement for implementation and continuous monitoring of what is to be achieved.	The legal system is an issue most of the time; the laws do not deter cybercriminals.

Table 7.1 discusses the validation of the proposed success factors found in the literature and the new factors derived during the interview discussion leading to the revised success factors for the developed CSRM implementation model. All the new factors received enough supporting evidence, but four did not gain common suggestion/support from the case organisations' explanations. Case studies B and D did not suggest organisational structure as a new factor. However, this study found strong validity put forward by case studies A and C. Hence, accepted as a factor since this study did not aim to apply critical success factors as the leading theory. What may be critical to an organisation might not be critical to another organisation. Change management factor found support from Case studies A and D but not mentioned in case studies B and C. Since two out of four expressed strong support, the factor is accepted.

Since Time has emerged in the literature as a reliable measure of success in IT project management (CSRM implementation is synonymous with a project), the response time factor is accepted. Likewise, response time as a factor gained support from Case studies A, B and D but not case study C, hence, accepted as a factor. Reasons include a time lag in any CSRM implementation programme might result in failure and adverse effects on the organisation's reputation in such a dynamic environment under study. The political environment affects the increasingly interconnected, complex socio-technical systems that metamorphose into cybersecurity risks and processes in Nigeria and another world social and economic systems. Hence, CSRM implementation success requires the collaboration between the political environment in terms of legal and regulatory governance systems, viable security policies, technological factors, and social factors.

7.3.2 Revised Success Factors Influencing CSRM Implementation Model in Large Organisations in Nigeria

This section revises and extends the success factors influencing CSRM implementation based on the research conducted in the four case organisations. The most recognisable outcome is a revised conceptual discussion model in the success factors influencing the CSRM implementation study. The identified success factors are consistent with the expectations of the conceptual model. Thirteen new success factors were identified from the empirical findings (from case studies A, B, C and D), as explained in Sections 6.3 (Figure 6.10) and Table 7.1. The empirical results show modifications to three factors (i.e., people, process, and organisation). Therefore, Figure 7.1 shows the revised success factors that influence CSRM implementation in large organisations in Nigeria.

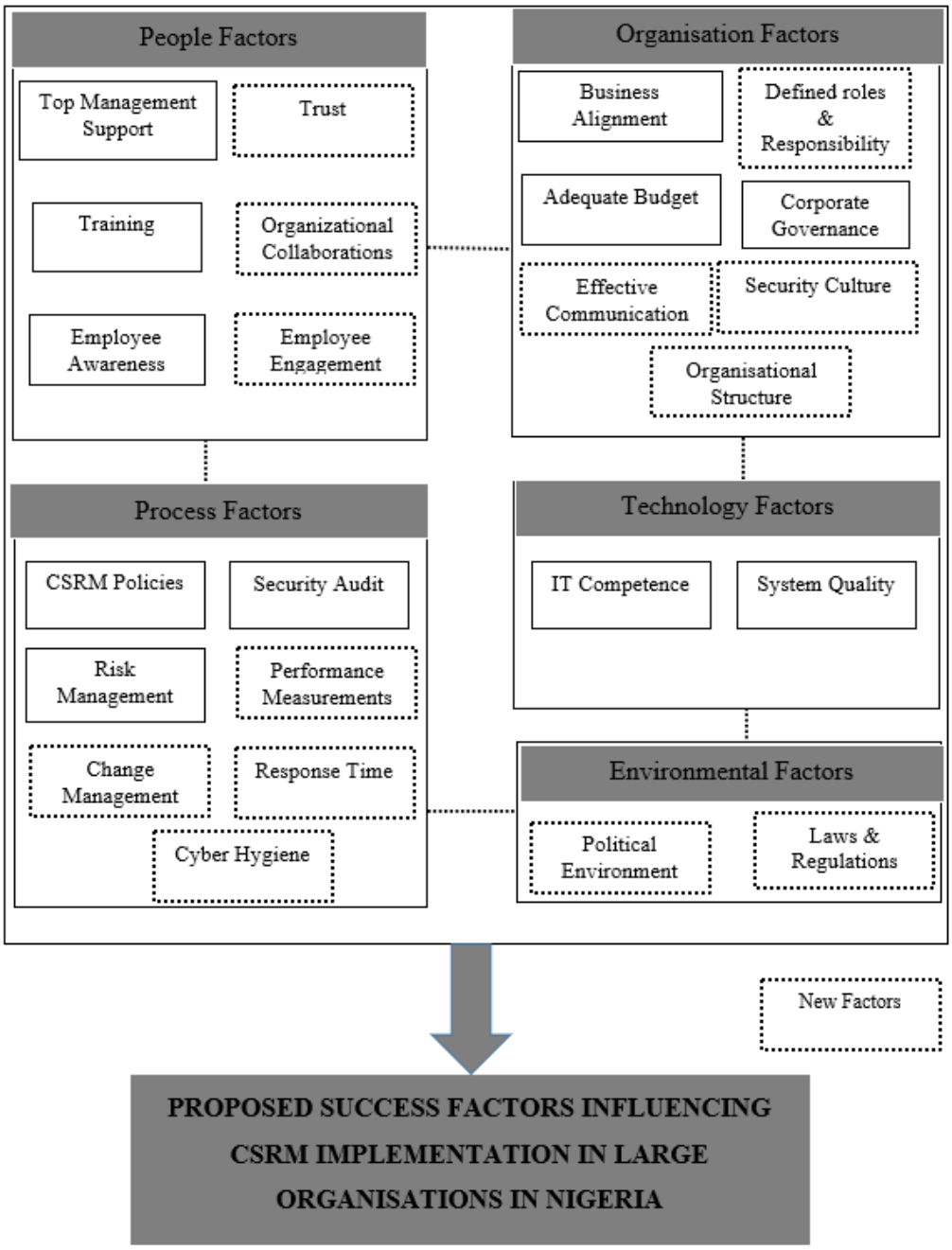

Figure 7.1: Revised Success Factors Influencing CSRM Implementation in Large Organisations

All the inquiry, explanations and features of compositions reflect reality and reliability. Supporting this evidence in figure 7.1 above, a successful organisation pursues effectiveness and efficiency through a change that incorporates internal and environmental factors to mitigate CSRM implementation challenges for competitive advantages in the business world. This success inspires the management to adopt and implement an open-system model. A more integrated

holistic view of enterprise-wide CSRM incorporates information security, people-asset security, process security, CS and some cases, national security organisational CSRM implementation success. ‘Unquestionably, the 'backbone of qualitative research is an extensive collection of data, typically from multiple sources of information in which new forms emerge that challenge traditional categorization’(Creswell and Poth 2016:34). Therefore, this research presents and advocates a revised conceptual model incorporating (the socio-technical and environmental factors) these different success factors but interrelated aspects of CSRM into a model of success factors for organisational CSRM implementation success in this chapter (Figure 7.1).

The model above highlights that Cyber Security Risk Management implementation is a process-based system that offers guidance to stakeholders on the enterprise's CSRM related activities. There are indications that many organisations have adopted and implemented CSRM. Implementation of CSRM involves an organisational CSRM change management process. Organisational CSRM implementation factors influence employees' duties, the work performance of aligning CSRM goals with business needs, the appropriate organisational and corporate governance structure, and the provision of adequate resources for implementing state-of-art technologies and necessary human competencies. Skilled, knowledgeable, and ethical system practitioners will ensure proper alignment of security requirements, practices and the effective use of technology enhancements and solutions within a regulatory framework and a favourable political environment. Therefore, the future organisational success plan should involve transforming the organisation from one state to the desired and enhanced through a comprehensive CSRM implementation success factors model.

7.4 Conclusion

The findings for (a) investigation of factors, (b) evaluation of factors, based on the four dimensions mentioned above (c) the development of success factors influencing CSRM implementation have been justified and presented. This chapter focused on revising the conceptual model proposed in Figure 3.1. The conceptual model was modified based on the empirical data presented and analysed in Chapter 6. The empirical evidence shows that the conceptual model's factors (Figure 3.1) should be considered while implementing CSRM in Nigeria and thirteen new factors. Trust, organisational collaborations, and employee engagement are among the new factors identified from empirical research related to the people factor. Trust is reported in all four case organisations, while employee engagement is suggested in Case studies A and B as factors influencing CSRM implementation in large organisations in Nigeria. Four

factors derived from the case organisations relate to the organisation. They are included in the revised conceptual model, namely organisational structure, CS-focused corporate culture, effective communication and defined roles and responsibilities reported in all four case organisations.

Case studies B, C, and D did not discuss organisational structure influencing CSRM implementation. The last four new factors derived from the case organisations related to process factor category, i.e., change management, cyber hygiene performance measures and response time. However, case studies B and C did not discuss change management; likewise, case study C did not discuss response time as factors influencing CSRM implementation in large Nigerian organisations.

The research presents a revised conceptual model in this chapter (Figure 7.1). The revised model proposes that five success factors themes influence CSRM implementation in large organisations in Nigeria. These factors categories include: (a) People; (b) Process; (c) Technological; (d) Organisational and (e) Environmental factors. In addition to these factor themes, the revised success factors model for CSRM implementation in large Nigerian organisations suggest factors (sub-themes) related to these categories:

- People Factors: Employee Engagement, Trust and Organisation's Collaborations).
- Process Factors: Performance Measurement, Response Time, Change Management and cyber Hygiene).
- Organisation Factors: Organisational Structure, Security Focused Organisational Culture, Defined Roles and Responsibilities and Effective Communication.
- Environmental Factors: Political Environment and Laws and Regulations.

All these factors assisted in understanding and analysis of the revised success factors influencing the CSRM implementation model. Thus, they contribute to the implementation success of CSRM in large organisations in Nigeria. The novelty of the success factors for the CSRM model presented in Figure 7.1 focuses on the following:

- The model consists of (a) factors influencing CSRM implementation in the case organisations, and (b) incorporates factors identified separately in previous studies. These success factors helped develop a conceptual model for CSRM implementation in large organisations in Nigeria.

- The model is not an exhaustive buzz. The consciousness of each success factor influencing CSRM implementation in large Nigerian organisations and more themes, processes, and approaches must be established.
- Finally, the model, partly free from the memories of social mathematics-covering laws, could serve as a tool for decision-making to support large organisations in Nigeria and allow practitioners and researchers to understand success factors for CSRM implementation in large organisations in Nigeria.

Chapter 8: Conclusions, Limitations and Future Recommendations

8.1 Introduction

The current chapter presents the research's overall summary based on four case studies' results and findings by revisiting the initial problem statement, objectives, and research questions. This chapter purposes achieving the following: (a) Ground the results in prior studies and conclude the research carried out in this thesis (b) highlight its achievements and contributions, (c) present the limitations in the research and (d) suggest areas for further research. Chapter 7 overviews the research conducted in this thesis and draws conclusions derived from the literature and empirical findings reported in Sections 8.3 and 8.4. The acclaimed novelty in this thesis is summarised in Section 8.5. The research achievement and scholarly implications to knowledge and practice are presented in sections 8.6 and 8.7.

Furthermore, reflect on the research process and present this research's limitations. This study suggests that these limitations should be considered when interpreting results. Finally, this chapter concludes and offers suggestions for further research in the challenging and fast-evolving research area of CSRM in large organisations in Nigeria.

8.2 Research Overview

Chapter 1 of this thesis began with the context of the research problem. Cyber Security Risk Management is a strategic issue in organisational management and business continuity. Organisations worldwide take advantage of information technologies for business growth and solve various organisational problems. However, large organisations in Nigeria experience challenges managing cybersecurity risks and threats due to a complex network of interdependent factors. This is because organisations partly commit to CSRM initiatives and inefficient practices due to insufficient knowledge and unawareness of the key factors contributing to its implementation success (Zammani and Razali 2016).

Studies on success factors in CSRM and related fields found a lack of in-depth research in CSRM implementation success that is not techno-centric. Literature found that there exist limited success factors models in large organisations. However, these models' validity and applicability cannot be easily transferred to this study context in large Nigerian organisations because they are non-generic. Few works of literature such as (Ogoh 2016; Okolo 2016; Ogu,

Ogu and Oluoha 2020) attempted to address these problems singly and at the organisational level, but the holistic study of these influential factors of CSRM implementation success remain under-researched in developing countries(Reza Hosseini et al. 2016).

This study found that success factors for CSRM implementation in Nigeria are gaps in literature requiring adequate attention. However, these models provided some understanding of CSRM implementation. This thesis presents the research to address the rising need to explore success factors for CSRM implementation in large organisations in Nigeria. Chapter 1 states that this thesis aims to *explore success factors influencing the implementation of CSRM in large Nigerian organisations.* It highlights the objectives and presents a general overview of the thesis outline in chapter 1.

Chapter 2 (background theory) reviewed the literature on CSRM in related disciplines in large organisations to address this thesis's aim and objectives. The reason was to provide an extensive overview, synthesis, and critical engagement with previous research to identify and analyse success factors for CSRM implementation in the existing literature. The objective is to understand and improve the current knowledge of the literature in this domain. The review offers extensive topic context and outlines the importance of novel research. The aim is to create study predictability using the information gathered from previous studies as inputs for this study (Section 2.6). The analysis identifies where the current research can contribute to a knowledge gap in the literature in optimising some socio-technical factors in Nigeria's large organisations.

The variables that influenced security success models and extended models in IS research were examined, perhaps closing the gap in CS research. After that, respond to the persistent emergence of many CS challenges and faulty CSRM implementation practices. To the best of the researcher's knowledge, the analysis of success factors for CSRM literature revealed that success factors for CSRM implementation are an under-researched area. There is a lack of broad-based theoretical and empirical research on success factors influencing CSRM implementation in large organisations in Nigeria for various reasons, as reported in Section 2.7. Lastly, the analysis extracts the research objectives outlined in section 2.8 of this thesis. Investigating the research problems derived from Chapter 2 is the focus of Chapter 3 (focal theory). In this regard, this study believes the research objectives are fundamental, necessitating a model of success factors for CSRM, the subject of this research was proposed in Chapter 3.

The proposed model contributes to large organisations and the CSRM implementation domain. Firstly, section 3.1 emphasised the need for a conceptual framework refined and adapted to identify and evaluate success factors for CSRM implementation in large organisations since the success factors from the literature review cannot be transferred easily to other sectors. Consequently, based on the review of conventional theories used in previous success factors studies in section 3.2, this study chose the Socio-Technical System theory approach to investigate success factors that influence CSRM implementation in large organisations in Nigeria (Section 3.2.1). Thus, Leavitt's model for IS success factors is the foundation for this study. Then, the factors identified in Chapter 2 served as the basis for proposed success factors influencing CSRM implementation in large organisations in Nigeria in section 3.4. However, these success factors present an original contribution at the conceptual level and need continuous refinement between theory and practice. Lastly, it concludes chapter 3 with an outline of the research issue in Table 3.1 for further investigation.

Chapter 4 (Data theory) outlined the research approach, methodology and design with the appropriate justifications. The developed and adopted research methodology (presented in Figure 4.1) justify selecting qualitative research approaches for data collection from four large organisations in Nigeria. The conceptual model (Figure 3.1) proposed in Chapter 3 was validated using the methodology explained in Chapter 4, advancing data and ideas through careful interpretations of the interviews and multiple views from four case studies organisations in Nigeria in Chapter 5 (Figure 3.7). Subsequent reports of the empirical evidence from the four case studies in large organisations in Nigeria, namely Case Study A, Case Study B, Case Study C and Case study D, are presented in Chapter 5. The chapter started with discussing and analysing the two pilot studies—progress with data analysis from the case organisations. Chapter 6 compares the similarities and differences between the analysis and the empirical findings from the evidence to investigate the conceptual model and the issues under investigation (Table 2.6). The "interpretive turn" led to further insights, understanding, and enriching the evaluation process's quality for the success factors influencing CSRM implementation in large organisations in Nigeria.

In Chapter 7, the empirical findings from the case organisations were extracted to (a) highlight the lessons learnt from this study (Section 7.2) and (b) revise the proposed success factors for CSRM implementation in large organisations in Nigeria (Section 7.3.1). As a result of the empirical findings and lessons learnt, the model was further synthesised, focusing on all the success factors influencing CSRM implementation and confirming the validity of the success

factors influencing CSRM implementation in their different classifications. Finally, it presents the revised model for success factors influencing CSRM implementation in large organisations in Nigeria (Figure 7.1). This model presents a valuable decision-making tool for large organisations during the CSRM implementation process. A note of caution regarding this proposed model is that it does not claim universality of thoughts applicable for all CSRM implementation decision-making scenarios. However, it presents socio-technical thinking as novel and potentially incites innovation, practical to study new success factors for CSRM implementation in large organisations in Nigeria.

8.3 Achieving the Aims and Objectives of the Study

Chapter 1 outlines the set objectives achieved, as discussed in the previous chapters, to accomplish this study's aims and objectives. Table 8.1 summarises and analyses these objectives in the following paragraphs.

Table 8.1: Achieving the Aims and Objectives of this Study.

Objectives	Chapter/Section
1	Chapters 1 and 2
2	Chapters 2 (Section 2.6, Table 2.5) and 3
3	Chapters 3 and 4
4	Chapters 5, 6, 7 and 8

- **Objective 1**: To critically review the success factors in CSRM literature and understand the area focusing on large organisations.

  Objective one provided adequate support to achieve the second research objective. A broad literature review of the research context provided an understanding of success factors themes and sub-themes for CSRM in large organisations. The literature review identified some research gaps and provided adequate support for subsequent exploration of success factors for implementing CSRM in Nigeria, which is currently lacking and further examined and investigated (Chapter 1 and Chapter 2).

- **Objective 2**: To identify and evaluate factors influencing CSRM implementation success in large organisations in Nigeria.

The literature's critical analysis on several success factors for CSRM models in related multi-disciplines identified different success factors for CSRM implementation (Table 2.5) singly and in large organisations in other regions and domains. The lack of a theoretical model for success factors for CSRM implementation was acknowledged, thereby identifying success factors that influence CSRM implementation in large organisations in Nigeria (Chapters 2 and 3).

- **Objective 3**: To develop and propose a model for success factors for CSRM implementation in large organisations.

  The pursuit of the aims and objectives so that the exploration targeted multiple case studies. As a result of the research conducted in Chapters 2 and 3 and the identified research objectives, the theoretical foundation for a conceptual model for success factors for CSRM implementation in Nigeria was proposed in Chapter 3. An appropriate research methodology for this thesis was justified in Chapter 4 to validate the proposed conceptual model (Chapters 3 and 4).

- **Objective 4**: To validate and evaluate the model within the practical arena and provide a novel contribution to large organisations and CSRM implementation in Nigeria.

  Chapter 5 and 6 present the analyses of the empirical data collected from 30 interviewees from the four case organisations in Nigeria, having validated the proposed model with the chosen research methodology. Thus, validating and evaluating the proposed model in chapter 3. The case studies' research findings were used to modify the proposed research model as deemed fit in Chapter 7. The revised model can be helpful as a decision-making tool while implementing CSRM in large organisations in Nigeria. Chapter 8 started with a summary of the thesis and concluded findings from the literature and empirical study. Finally, stated the novel contributions of the research.

The developed novel model linking socio-technical theory for addressing the research problem concerning success factors influencing CSRM in large organisations in Nigeria helped achieve the objectives mentioned above. When turning a systemic lens upon the organisation's nature, it is possible to perceive that a higher order of complexity is involved. As Mumford (2006) points out, organisations can be perceived as dynamic and open systems-elements continually entering, interacting, and leaving over time. Cybersecurity risk management is a dynamic phenomenon that

needs constant change for CSRM implementation success. The socio-technical approach helped explain the success factors model's appropriateness for CSRM implementation practices within large organisations' practical reach in Nigeria. Hence, there are relatively few differences in the factors and approaches though similar, based on the organisations' innovation or strategies in working practices, attention to collaborative activities, processes, and human desire to achieve excellence.

This thesis aims not to develop a theory of organisation in a comprehensive complex phenomenon and uncertain environments but to use an analytic framework to explore success factors for CSRM implementation and interpret the concept of CSRM implementation success. The only difference in this study is how the theory and concepts justify the need for this study, the type of organisations included, the analysis and subsequent data interpretation. The insights are drawn from systems thinking to guide the arguments. The data analysis reveals some local contextual factors and assumptions important in a conceptual model to support developing countries.

Hence, this research has demonstrated the value of advancing new areas of thinking in the new domain, thereby contributing to theory and practice. Each contribution from this research originated from the different phases of this study ranging from (a) the background information that established the study context discussed in Chapters 1 to 3, (b) to the chosen research methodology discussed in Chapter 4, (c) through the design and conduct of case studies of purposeful samples to gain varieties of different perspectives on the research objectives discussed in Chapters 5, (d) the analyses of the empirical findings reported in Chapters 5 and 6, (e) Lastly, the development and presentation of the revised model in Chapter 7.

8.4 Key Findings of this Thesis

In agreement with Yin 2018, the main focus of this research, success factors influencing cybersecurity risk management, is a contemporary phenomenon instead of historical necessitating, how and why questions typical of a rigorous case study research. How can one relate experiences in a survey? The interview questions were more exploratory, tracing operational processes over time rather than mere frequencies or incidences. Investigating how and why these organisations are successful led to more assurance of multiple case studies and documentary information /evidence supplied by some organisations to strengthen their explanations.

According to Max Weber, qualitative researchers often take ‘understanding’ rather than ‘explanation’ as the social sciences' goal. Instead of assuming that the causes and effects of human actions and experiences can and should be studied objectively using natural sciences (measurement, control of variables, standardised procedures) (Burrell and Morgan 2017). Qualitative researchers often (though not always) take an interpretivist approach in understanding the meanings that people attach to their experiences and practices (Burrell and Morgan 2017). The assumption is that these meanings will vary and develop differently in different contexts (Creswell and Creswell 2018).

Numerous IS researchers have argued for the need for a more comprehensive selection of methodologies to gain new detailed insights and discovery. That is undoubtedly a noble view others share (Walsham 1995; Weill and Olson 1989). Therefore, the philosophical and social worlds investigated are not assumed to be straightforwardly predictable and governed by general laws of cause and effect (Gertz 2004). In this position, qualitative data analysis is viewed as an interpretation. Just as research participants may make different meanings about CSRM implementation successes in their organisations, the researcher constructs one of many possible interpretations of the participants' meaning (Fujs, Mihelič and Vrhovec 2019). On this basis, the factors influencing CSRM implementation success are interpreted within a socio-technical model of organisational change that includes people, process, technology, and organisational factors.

It is worth regularly exploring and documenting CSRM implementation success factors for replication in future CSRM / IS projects in the organisational environment. The findings support that reflecting on implementation success factors is a priority in practice attained through focusing on people, processes, and technological systems. The key findings are presented as short but complete statements of easy-to-read important facts based on the participant's ability to articulate themselves. Making it easy to draw the reader's attention to important information rather than read word for word that could be boring. The summary of key findings that emerge from unearthing new insights from the data with several iterations revealed the followings:

- **Findings 1**: Limited research concerning success factors for CSRM in large organisations is discussed in chapters 1 and 2 with confirmation from the empirical study conducted in large organisations in Nigeria.
- **Findings 2**: The critical engagement with literature and what it means to be scholarly in academic work through an extensive overview of the success factors for CSRM in related existing literature helped this study identify the persistent emergence of many CSRM

challenges large organisations face. Further, to close the lacuna in CSRM research in large organisations by identifying and evaluating success factors for CSRM implementation as empirically confirmed in Chapters 5 and 6.

- **Findings 3**: It was found that there have been many research topics on success factors and extensions of models after developing the IS success model. The CSRM domain has not attracted significant interest because much attention is on securing information systems security software and hardware capabilities. This research benefits from the comprehensive literature review. It summarises the success factors in a cohesive variety of prior related research in CSRM and its associated fields from both singular and organizational-wide studies to focus and understand the success factors for CSRM implementation. However, these success factors' validity and applicability may not be generalised and may not influence CSRM implementation success in large Nigerian organisations. As such, they may not be easily transferred to this study context. The aim is to create study predictability using the information gathered from previous studies as inputs for this study. Then, it leads to the identification and proposal of new success factors forming the input for the future validation of CSRM implementation in large organisations in Nigeria. These factors were validated to certify that they are influential and applicable, with thirteen new success factors identified by induction in the case organisations.
- **Findings 4:** Literature recommended using socio-technical views as the appropriate basis for analysis purposes and intervention strategies for practical work. Chapter 3 explored the opportunity and proposed the conceptual model for success factors for CSRM implementation in large organisations. Chapters 5 and 6 presented the empirical study to validate the proposed success factors for CSRM implementation with the revised model in Chapter 7. The need to articulate and optimise such factors for CSRM implementation success from the socio-technical perspective is evident as deemed fit. The extended Socio-Technical Theory in success factors for CSRM implementation indicates that each of the themes is insufficient when employed without the others in addressing the issues that pertain to achieving CSRM implementation success. As such, there is an appreciable 87% acceptance to receive the study's full report. More importantly, the study affirms that the model can be used as a decision-making tool to assist organisations in CSRM implementation efforts and practices.
- **Finding 5:** The literature review revealed a sparse conceptual model describing the link between CSRM implementation success factors and CSRM practices.

In summary**,** this study's evidence helped understand the components of CSRM implementation in Nigeria through the socio-technical approach considering the socio-technical factors-technology, organisation, people and process, environmental factors. In the last decade, political environment/national politics has become an inter-disciplinary weapon woven into every fabric of developing and developed countries ranging from cyber security policies to laws and regulations. The political environment exacerbates cyber security risks and incidents in many organisations by malware kings. Hence, in a more competitive and more targeted business environment, the top management must operationalise and interplay socio-technical factors with the political environment to produce a thriving relationship for CSRM implementation success.

In conclusion, the joint optimisation of the business goals and objectives aligned with CSRM implementation needs with appropriate corporate governance structure and strategies must inspire CSRM culture. Employing sets of CSRM policies, processes and practises with various technological tools and controls engage, guide and influence people with multiple skills, attitudes and trust through continuous updated awareness and training programs within an enabling defined legal and political environment. This system (organisation and CSRM implementation framework) is expected to witness new changes to the implementation process in line with the dynamic nature of evolving CS risks and threats. Consequently, a synergy between the organisation, people, technology, process, and environmental factors is indispensable for any CSRM implementation initiative to be effective and successful. A reconfiguration of thoughts-CSRM implementation success combines proactive and future proof factors and strategies.

8.5 Research Contribution and Novelty

The contribution of this research is considered with a broader, more comprehensive definition of success. This study explored multiple dimensions with the potential to demonstrate the value in advancing socio-technical ways of thinking in a diversified manner through the components of this thesis. This study has made a novel contribution to the evolving area of success factors for CSRM implementation in large organisations, specifically in Nigeria, insufficiently revealed in literature and extended the frontiers of the knowledge in cybersecurity and risk management literature. The research asserts novel contributions in seven ways:

- 1st Contribution: Innovation in the investigation (Figure 3.1), validation (Tables 7.1) and identification of new factors (i.e., Trust, Change Management, Security focused Culture, Political environment, Employee Engagement and many more discussed in section 6.3

and section 6.4) for success factors influencing CSRM implementation in a large organisation in Nigeria *(Satisfying research problem 1 – Table 7.1)*.

- 2nd Contribution: The first of its type. This study coherently extended the Socio-Technical approach to the success factors for CSRM implementation in Nigeria. The findings help focus on success factors that large organisations should reflect on during their strategic CSRM implementation processes. Although existing literature has extended socio-technical theory in different contexts (Bednar, Welch and Milner 2016; Carayon et al. 2015; Kayworth and Whitten 2010; Palvia, Sharma and Conrath 2001), a detailed compilation of factors for large organisations to implement CSRM successfully is lacking.
- 3rd Contribution: The socio-technical approach identifies and mitigates cybersecurity risks through a conceptual framework that promotes a broad range of success factors that address diverse, complex issues and world challenges into a comprehensive enterprise-wide CSRM implementation success model.
- 4th Contribution: The thesis accommodates and presents qualitative evidence of exhaustive empirical accounts of lower, middle and top management levels in different ways and classifications to varying organisations with regards to Organisational, People, Process, Technological, Environmental factors, and their control activities that large organisations should consider in deciding to implement CSRM success. Also, it provides an account of successes of CSRM implementation that have been achieved in a few large organisations where research is lacking.
- 5th Contribution: It is by no means an exaggeration to state that this study addresses some of the criticisms of socio-technical systems theory. It extends beyond the axis of quantitative analysis. Still, a study of qualitative evidence adds value to the important role of systematic reviews of practice, strategic decision-making, and policies that will benefit CSRM implementation managers, cybersecurity, and risk management managers.
- 6th Contribution: Evaluating each factor's success in CSRM implementation through qualitative evidence and interventions that directly inform practices concerning the changing nature of technology and work practices to mitigate the CSRM domain complexities.
- 7th Contribution: Finally, the above-mentioned contributions led to a novel model of success factors for CSRM implementation in large organisations, particularly in Nigeria. The model could serve as a precursor and a helpful decision-making tool that assists practitioners and senior management in large organisations while implementing CSRM (*fulfilling this research aim*).

The summary of the research contributions and novelty is highlighted in table 8.2 below:

Table 8.2: Summary of Research Contributions and Novelty

Novelty	Areas of Contributions	Research Novelty	Research Contribution
Identifying and validating new success factors for CSRM implementation in large organisations in Nigeria	Investigation and validation of success factors influencing CSRM implementations in large organisations in Nigeria.	-	✓
	Identification of new success factors through the extension of the Socio-Technical approach through empirical research.	✓	✓
	Identification of new success factors through empirical research in case organisations using thematic analysis	✓	✓
Evaluating success factors influencing CSRM implementation in large organisations in Nigeria.	Evaluation of the success of each factor in CSRM implementation in large organisations in Nigeria.	✓	✓
Novel Model of Success Factors for CSRM Implementation in large organisations in Nigeria	A novel combination of success factors that influence CSRM implementation in Nigeria determines each factor's effectiveness and control activities.	✓	✓
	Increase awareness of success factors for CSRM implementation to address a broader range of complex issues and global challenges and contribute to more effective work.	✓	✓

8.6 Research Achievement

The previous section highlights the components of the contributions and originality of this thesis. The research achieves the kinds of scholarship defined by Boyer et al. (2015). “Discovery scholarship” at its highest leads to the development of knowledge in the intellectual environment of the university to resolve the irrepressible need of human beings to address the unknown success factors for the implementation of CSRM in large organisations in Nigeria.

The “integration scholarship”, which means interpretation, is closely related to exploration. First, it includes discovering the boundaries where fields intersect. The integration scholarship interprets what the results mean- provide a more comprehensive, more thorough understanding through critical analysis and interpretation—based on careful credibility that leads from information to knowledge and perhaps wisdom. This interdisciplinary study is, in reality,

imperative, as conventional disciplinary categories prove to confine by pushing new knowledge topologies, by fitting research into broader intellectual trends.

Overall, this study is a rare exhilaration that derives from innovative concepts aimed at supporting large companies in their strategic planning and decision-making processes to achieve success in implementing CSRM. To achieve this purpose, this study proposed and validated a novel model (Figure 3.1) of success factors influencing CSRM implementation in practice in four large organisations in Nigeria (Case Studies A, B, C and D).

Though data gathering occurred in Nigeria, the success factors could be applicable in broader contexts. The model may serve as a valuable reference for organisations anxious about combating the menace of faulty CSRM implementation practices. Therefore, benefiting the key decision-makers and practitioners in large organisations necessitates further study. This research is also helpful for comparative study in other developing economies and other environments with social, cultural, and economic differences.

8.7 Research Implications

Implications to Theoretical Knowledge

This research differs from previous studies in Nigeria and other developing countries, emphasising CSRM and its implementation success. The socio-technical approach coherently extends the frontiers of knowledge of CSRM implementation success factors insufficiently revealed in cybersecurity and risk management literature. There were gaps in prior studies until recently; previous research such as Dugguh and Diggi (2015) and Gana, Shafi'i and Ojeniyi (2019) have identified some factors singly and disjointed in CS and risk management practices. Others suggest that critical CS solutions and measures rarely succeed at implementation in Nigeria (Oforji, Udensi and Ibegbu 2017; Okolo 2016).

There has been a propensity to concentrate on technical factors for CSRM without social factors, and its implementation success is scarcely implied in the Nigerian context. For example, essential technological measures such as system quality and trust, organisational collaborations, security culture and other people factors are ignored. Hence, evaluating CS implementation success factors becomes a necessary consideration with more extensive attention in an organisation with numerous measures and features put into the efforts and processes.

Therefore, the research provides a conceptual success factors model and their relationships and contributes to increasing the body of success factors for CSRM implementation knowledge in a new context in large organisations in Nigeria. Thereby moving the literature from the challenges and problem rhetoric to success repetitions.

The advantage of taking a holistic approach is that CSRM success encapsulates the effective coordination and the synergies between the interrelated socio-technical-organisational success factors for CSRM implementation examined, organised, and conceptualised as comprehensive logical factors. The theories underpinning prior studies such as system thinking, game theory, organisational theory, and IS success model reveal no comprehensive model to find out the success factors affecting the successful implementation of CSRM in a more holistic comprehensive view. By adding the knowledge transfer of risk management to cybersecurity, the study provides additional insight that allowed the use of the socio-technical theory combined with the Leavitts model and IS to cover all the factors initially discovered during the study.

Implications to Practice/Managers

This research contributes valuable insights to CSRM implementation practice by providing a success factor model that can be used as a precursor and a decision-making tool. It can assist security managers, risk managers, security consultants or other managers to tailor, develop, optimise the CSRM implementation process fit for organisations. The instructive use of a universal framework for CSRM and the level of knowledge are relatively scarce. CSRM is increasingly being adopted and implemented onto an organisation, rather than other socio-technical CSRM models emerging from organisations. Increased awareness of success factors may address the CSRM complex issues and global challenges. The model may help execute and achieve CSRM implementation objectives, improve CSRM implementations success rate and promote cyber peace.

The study analyses the success factors and has provided evidence to improve CSRM implementation success in Nigeria. Although numerous studies have identified CS and risk management's challenges, about 90% of prior studies are quantitative, with little qualitative analytical attention paid comprehensively to success factors. Therefore, no or few factors were coming up. However, latest studies such as Alawonde (2020), Fujs, Mihelič, and Vrhovec (2019) and Wang and Nnaji (2020) request for more qualitative studies to be able to understand what happens in practice. This piece of work in the interpretive tradition, rich and in-depth coverage

and analysis of the factors and the relationships between them and the conclusions are relevant today and make a more meaningful contribution. More elements are coming up with the maturity and evolutions of the field arising out of the insights from several organisational implementation success case studies under the headings of content, social context, and socio-technical processes challenging to capture through a quantitative study. Hence, the qualitative research findings will enable IT managers and CS risk management experts in large organisations in Nigeria to better understand, implement, evaluate, and explore the factors for CSRM implementation success and their impacts.

The thesis comprises valuable information on 'why' and 'how' success factors for CSRM implementation that can assist CISOs, executive management, academics, and other small and large organisations to understand CSRM implementation success factors and processes. Although the empirical study was primarily in organisations in Nigeria, a developing country, its subjectivity and the construction of knowledge of each success factor make it globally relevant since CSRM has no geographic boundary.

8.8 Research Limitations

The work has some potential weaknesses as limitations. The most important limitation of this study lies in focus on large organisations in Nigeria, and the samples of the study have only investigated large organisations in Nigeria. Large organisations are predominant primary adopters of technological innovations for business growth, coveted prime targets of cybercriminals for scrupulous gains and many more discussed in Section 4.5.3 of this thesis. Also, caution must be exercised as the structure, security focus and operations of large organisations in Nigeria differ. For example, large public organisations in Nigeria are different from private E-retail and financial organisations in Nigeria. Therefore, the empirical findings might not be generalised but restricted to large organisations in Nigeria. However, the research findings show that some of the success factors in large organisations in Nigeria were comparable to those influential in most countries' geographic locations.

Also, finding a more significant number of interviewees who were not reluctant to freely discuss or relate their experience on a sensitive topic as success factors for CSRM implementation proved very difficult. Hence, there are limitations and critics of the sample size of case studies common to qualitative case studies and the inability to generalise the study result. Nevertheless, this study overcomes these criticisms by drawing from other studies that have used case studies to

investigate success factors perspectives (Al-Awadi and Renaud 2007; Zammani and Razali 2016) and other documents as data sources. Often multiple case studies are considered more trustworthy with convincing results (Yin 2003) with the interviews leading to more realities (Bryman 2015) mainly for insights into the factors within intricate settings in need of an in-depth understanding of the stories behind the outline of success factors and the results in a relaxed way (Neale, Thapa and Boyce 2006). These reasons justify using multiple case studies in this study.

The use of qualitative evidence for data collection discussed in Chapter 4 advances rich and contextual data and ideas through careful interpretations of the social meaning of words, holistic understanding of actions and views intellectually found in interaction with a purposive sample size in large organisations in Nigeria. As is well known, the interpretation of the collected data from the context of four case studies organisations was challenging and without a level of bias challenging to control. The disadvantage of using a qualitative method is the researcher's downside of spending an extended period in data collection and analysis.

Despite this method's limitations, the bias permits gathering information from a holistic study of a complex web of social-technical interactions, social actions, and social meanings from multiple case studies for an extended period, as explained in Chapter 4. Additionally, it permits comparing empirical data gathered with reflectivity and flexibility to meet unexpected issues and results. Member checking and re-confirming of interviewees' results address this study's bias concerning the environmental factors that the participants argued could be both success factors and challenges. Developing a model of success factors influencing CSRM implementation with the activities/control factors is extremely hard but worthwhile in addressing this study's bias.

Inevitably, the researcher could not access other large organisations and other sectors due to confidentiality issues, the topic's sensitivity, and the country's peculiar state of cybercrime activities.

8.9 Future Research Recommendations

This research has thrown up some questions in need of further investigations, namely:

- **Recommendation 1:** The result of this research may not be generalized due to large organisations' organisational structure, culture, and operational activities in other geographic locations of the world. Future research should revalidate the model to confirm

that the success factors will be similar in different geographic areas and include other non-financial organisations in Nigeria, such as telecommunication.

- **Recommendation 2**: The conceptual model considered large organisations' distinctive characteristics in Nigeria's four case organisations. Cybersecurity is evolving, social realities growing, new ideas and concepts evolving to match the pace of innovations in problems and solutions. There is a need to reevaluate the success factors and suggest that this study may serve as a foundation for further studies.
- **Recommendation 3**: The study has also identified the new success factors that are controversial and individual in large organisations. Future studies could examine their applicability in more sectors.
- **Recommendation 4**: The research has found success factors for CSRM implementation in large organisations in Nigeria from the interpretivist epistemology due to limitations peculiar to the Nigerian context and resources. Future research could enhance the result's quality by assessing the relationship between the factors in a more comprehensive quantitative analysis.
- **Recommendation 5**: Theory suggests that more socio-technical factors are not covered in this study due to more concentration on social and technical factors within a bounded organizational setting. Future interdisciplinary research could investigate these factors and other influential socio-economic factors such as the political environment that will help inform policies and decision-making towards achieving more CSRM implementation success at the organisational and national level.
- **Recommendation 6**: Finally, the research could identify and validate success factors for CSRM implementation in SMEs in Nigeria. The objective is to compare the CSRM implementation practices with an implication for social change and practices. The literature revealed that a versed majority are reluctant to explore the gains of technology innovation for business growth due to the constant challenges of CSRM all over the world.

8.10 Concluding Remarks

This thesis compiles a curious research project from four large organisations over four years. This research has contributed to the knowledge and practice of cybersecurity risk management and its implementation in the extant cybersecurity and risk management domain. Moreover, it has made significant implications to the researcher and all stakeholders in completing the PhD research.

This research has an invaluable opportunity that revolutionises the researcher in all areas of life and career. It helped rediscover and develop hidden skills such as people and time management skills, interview skills, and resilience amidst all challenges, including health, enhancing her academic background with unique organisational experience. These vital collaborations and partnerships between industries/businesses, academia, leaders, regulators and policymakers will enhance her future academic career and assist her in conducting relevant and rigorous research.

The lower, middle and senior management of the case organisations felt fulfilled in contributing to knowledge in the cybersecurity domain with the cordial relationship, increased knowledge base from the exchange of ideas and information derived from their collaboration with the research project.

Cybersecurity risk management is a multi-disciplinary field. Success factors for CSRM implementation should bring together knowledge, skills, and expertise from multiple disciplines. Colleagues at various departments at Coventry University benefitted from the lessons learned given the enormous efforts and commitment put in throughout conducting the research and writing the thesis. More importantly, those working on related topics share ideas, knowledge, encouragement, and insights.

Hence, this thesis has successfully revealed an area capable of opening more opportunities for research and teaching in cybersecurity/Is discipline, social sciences and strategic management disciplines and more collaboration with the industry for the centre for business and society at Coventry University.

The inevitable ambiguity in CSRM implementation success factors is now explored in this thesis, with its contribution to knowledge and practice.

References

Abdul-Rasheed, S. L., Lateef, I., Yinusa, M. A. and Abdullateef, R. (2016) 'Cybercrime and Nigeria's External Image: A Critical Assessment'. *Journal of Pan African Studies*, 9 (6), 119-133

Achumba, I. C., Ighomereho, O. S. and Akpor-Robaro, M. O. M. (2013) 'Security Challenges in Nigeria and the Implications for Business Activities and Sustainable Development'. *Journal of Economics and Sustainable Development*, 4 (2)

Agarwal, N. and Rathod, U. (2006) 'Defining 'Success' for Software Projects: An Exploratory Revelation'. *International Journal of Project Management*, 24 (4), 358-370

Ahmed, N. and Matulevičius, R. (2014) 'Securing Business Processes Using Security Risk-Oriented Patterns'. *Computer Standards & Interfaces*, 36 (4), 723-733

AIRMIC, A. and Irm, A. (2010) 'Structured Approach to Enterprise Risk Management (ERM) and the requirements of ISO 31000'. *The Public Risk Management Association, London, UK*

Ajah, B. O. and Chukwuemeka, O. D. (2019) 'Neo-Economy and Militating Effects of Africa's Profile on Cybercrime'. *International Journal of Cyber Criminology*, 13 (2)

Akinwumi, D. A., Iwasokun, G. B., Alese, B. K. and Oluwadare, S. A. (2017) 'A Review of Game Theory Approach to CSRM'. *Nigerian Journal of Technology*, 36 (4), 1271-1285

Aladenusi T. (2020) [online] available from<https://www2.deloitte.com/ng/en/pages/risk/articles/nigeria-cyber-security-outlook-2020.html> [10 July 2020]

Aladenusi T. (2021) [online] available from<https://www2.deloitte.com/ng/en/pages/risk/articles/nigeria-cyber-security-outlook-2021.html> [28 January 2021]

Al-Awadi, M. and Renaud, K. (eds.) (2007) *IADIS International Conference e-Society*. 'Success Factors in Information Security Implementation in Organisations'

Al-Awadi, M. (2009) *A study of employees' attitudes towards organisational information security policies in the UK and Oman.* [online] Doctoral thesis, University of Glasgow

Alawonde, K. O. (2020) *Tailored Information Security Strategies for Financial Services Companies in Nigeria*. [online] Doctoral dissertation, Walden University

Ale, B., Aven, T. and Jongejan, R. (2009) 'Review and Discussion of Basic Concepts and Principles in Integrated Risk Management'. *Reliability, Risk and Safety: Theory and Applications*, 421-427

Allen, B., Kelly, T., Loyear, R., Poole, A., Awojulu, A., Kmetetz, A., Rakotomavo, M., Wang, Z., Xu, H., Xu, M. and Yuan, H. (2018) 'Security Risk Governance: A Critical Component to Managing Security Risk'. *The Journal of Applied Business and Economics*, 20 (1), 132-146

Althonayan, A. and Andronache, A. (2019) 'Resiliency under Strategic Foresight: The effects of Cybersecurity Management and Enterprise Risk Management Alignment'. In *2019 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (Cyber SA)*, held at IEEE, 1-9

Alvesson, M. and Sandberg, J. (2011) 'Generating Research Questions through Problematization'. *Academy of Management Review* 36 (2), 247-271

Amarilli, F., Van Vliet, M., and Van den Hooff, B. (2017) 'An Explanatory Study on the Co-Evolutionary Mechanisms of Business It Alignment'

Aminu, S. A. (2013) 'Challenges Militating against Adoption of Online Shopping in Retail Industry in Nigeria'. *Journal of Marketing Management*, 1 (1), 23-33

Andersen, T. J., Garvey, M. and Roggi, O. (2014). Managing Risk and Opportunity: The Governance of Strategic Risk-Taking.: OUP Oxford

Ani, U. D., He, H. and Tiwari, A. (2019) 'Human Factor Security: Evaluating the Cyber Security Capacity of the Industrial Workforce'. *Journal of Systems and Information Technology* 21 (1), 2-35

Appelbaum, S. H. (1997) 'Socio-Technical Systems Theory: An Intervention Strategy for Organisational Development'. *Management Decision* 35 (6), 452-463

Armstrong, C. S., Blouin, J. L., Jagolinzer, A. D. and Larcker, D. F. (2015) 'Corporate Governance, Incentives and Tax Avoidance'. *Journal of Accounting and Economics* 60 (1), 1-17

Ashenden, D. and Sasse, A. (2013) 'CISOs and Organisational Culture: Their Own Worst Enemy?'. *Computers & Security*, 39 396-405

Atoum, I., Otoom, A. and Abu Ali, A. (2014) 'A Holistic Cyber Security Implementation Framework'. *Information Management & Computer Security* 22 (3), 251-264

Aven, T. (2012) 'Foundational Issues in Risk Assessment and Risk Management'. *Risk Analysis*, 32 (10), 1647-1656

Aven, T. and Zio, E. (2014) 'Foundational Issues in Risk Assessment and Risk Management'. *Risk Analysis*, 34 (7), 1164-1172

Avgerou, C. and Walsham, G. (2017) *Information Technology in Context: Studies from the Perspective of Developing Countries: Studies from the Perspective of Developing Countries*: Routledge

Aviad, A., Wecel, K., and Abramowicz, W. (eds.) (2018) *International Conference on Cyber Warfare and Security*. 'Semantic Risk Assessment for Cybersecurity': Academic Conferences International Limited

Bannerman, P. L. (2008) 'Risk and Risk Management in Software Projects: A Reassessment'. *Journal of Systems and Software*, 81 (12), 2118-2133

Baskerville, R., Rowe, F., and Wolff, F. (2018) 'Integration of Information Systems and Cybersecurity Countermeasures: An Exposure to Risk Perspective'. *ACM SIGMIS Database: The DATABASE for Advances in Information Systems* 49 (1), 33-52

Bassellier, G., Reich, B. H. and Benbasat, I. (2001) 'Information Technology Competence of Business Managers: A Definition and Research Model'. *Journal of Management Information Systems*, 17 (4), 159-182

Baxter, G. and Sommerville, I. (2011) 'Socio-Technical Systems: From Design Methods to Systems Engineering'. *Interacting with Computers*, 23 (1), 4-17

Bazeley, P. a. (2013) *Qualitative Data Analysis with Nvivo*. Second edition / Pat Bazeley & Kristi Jackson. edn.

Beasley, M. S., Branson, B. and Hancock, B. V. (2020) 'The State of Risk Oversight: An Overview of Enterprise Risk Management Practices'. *NC State Pool College of Management, Enterprise Risk Management Initiative*. [online]. available from<erm.ncsu.edu/library/article/2020-the-state-of-risk-oversight-an-overview-of-erm-practices> [28 February 2021]

Bednar, P. M. and Welch, C. (2019) 'Socio-Technical Perspectives on Smart Working: Creating Meaningful and Sustainable Systems'. *Information Systems Frontiers*, 1-18

Bednar, P. M., Welch, C., and Milner, C. (2016) 'Excellence in Practice through a Socio-Technical, Open Systems Approach to Process Analysis and Design'. *International Journal of Systems and Society (IJSS)* 3 (1), 110-118

Ben, A. (2009) 'Risk', Routledge Ltd

Ben-Ari, A. and Enosh, G. (2011) 'Processes of Reflectivity: Knowledge Construction in Qualitative Research'. *Qualitative Social Work* 10 (2), 152-171

Bendovschi, A. (2015) 'Cyber-Attacks – Trends, Patterns and Security Countermeasures'. *7th International Conference On Financial Criminology 2015, 7th ICFC 2015, 13-14 April 2015, Wadham College, Oxford University, United Kingdom*, 28 24-31

Bergeron, F. and Begin, C. (1989) 'The use of Critical Success Factors in Evaluation of Information Systems: A Case Study'. *Journal of Management Information Systems* 5 (4), 111-124

Bergström, E., Lundgren, M. and Ericson, Å. (2019) 'Revisiting Information Security Risk Management Challenges: A Practice Perspective'. *Information & Computer Security*

Bharati, P. and Chaudhary, A. (2006) 'Product Customization on the Web: An Empirical Study of Factors Impacting Choiceboard User Satisfaction'. *Information Resources Management Journal (IRMJ)* 19 (2), 69-81

Biener, C., Eling, M. and Wirfs, J. H. (2015) 'Insurability of Cyber Risk: An Empirical Analysis'. *The Geneva Papers on Risk and Insurance Issues and Practice* 40 (1), 131-158

Bissell, K. (2013) 'A Strategic Approach to Cyber Security: As Cybercrime Grows Faster Than Companies Can Defend against, It is Time for a Serious Discussion on Cyber Security. Though Many Are Calling for Federal Standards and Regulations--Which May Be a Matter of Time--in Their Absence, Organisations Should Transform How They Think About Cyber Security'. *Financial Executive*, 29 (2), 36-42

Bobbert, Y. and Mulder, H. (2015) 'Governance Practices and Critical Success Factors Suitable for Business Information Security'. in (ed.) *2015 International Conference on Computational Intelligence and Communication Networks (CICN)*. held at IEEE, 1097-1104

Boell, S. K. and Cecez-Kecmanovic, D. (2015) 'On Being 'Systematic'in Literature Reviews.' in *Formulating Research Methods for Information Systems*. ed. by Springer, 48-78

Bojanc, R. and Jerman-Blažic, B. (2008) 'An Economic Modelling Approach to Information Security Risk Management'. *International Journal of Information Management*, 28 (5), 413-422

Borum, R., Felker, J., Kern, S., Dennesen, K. and Feyes, T. (2015) 'Strategic Cyber Intelligence'. *Info and Computer Security* 23 (3), 317-332

Boyatzis, R. E. (1998) *Transforming Qualitative Information: Thematic Analysis and Code Development*. Thousand Oaks, Calif; London: Thousand Oaks, Calif.; London: Sage Publications

Boyer, E. L., Moser, D., Ream, T. C. and Braxton, J. M. (2015) *Scholarship Reconsidered: Priorities of the Professoriate*. Hoboken: John Wiley & Sons, Incorporated

Boynton, A. C. and Zmud, R. W. (1984) 'An Assessment of Critical Success Factors'. *Sloan Management Review* 25 (4), 17-27

Brauner, P., Philipsen, R., Valdez, A. C. and Ziefle, M. (2019) *Human Interaction Under Risk in Cyber-Physical Production Systems*.: Springer Verlag

BRC (2020) [online] available from<https://brc.org.uk/media/676134/cyber-resilience-toolkit-for-retail.pdf > [19 November 2020]

Brinkmann, S. and Kvale, S. (2018) *Doing Interviews*. Sage

Bryman, A. (2015) *Social Research Methods*.: Oxford university press

Bryman, A. and Bell, E. (2015) *Business Research Methods*.: Oxford University Press, USA

Bullen, C. V. and Rockart, J. F. (1981) 'A Primer on Critical Success Factors'

Bunker, G. (2012) 'Technology is Not enough: Taking a Holistic View for Information Assurance'. *Information Security Technical Report* 17 (1), 19-25

Burrell, G. and Morgan, G. (2017) *Sociological Paradigms and Organisational Analysis: Elements of the Sociology of Corporate Life*: Routledge

Caldwell, T. (2016) *Making Security Awareness Training Work*. Oxford, Eng.

Camilleri, E. a. (2016) *Project Success: Critical Factors and Behaviours*

Camillo, M. (2017) 'Cybersecurity: Risks and Management of Risks for Global Banks and Financial Institutions'. *Journal of Risk Management in Financial Institutions* 10 (2), 196-200

Caralli, R. A., Stevens, J. F., Young, L. R. and Wilson, W. R. (2007) *Introducing octave allegro: Improving the information security risk assessment process*

Carcary, M., Renaud, K., McLaughlin, S. and O'Brien, C. (2016) 'A Framework for Information Security Governance and Management'. *It Professional*, 18 (2), 22-30

Central Bank of Nigeria (2018) [online] available from< https://www.cbn.gov.ng/out/2018/bsd/risk%20based%20cybersecurity%20framework%20final.pdf > [23 August 2019]

Chabinsky, S. (2014) 'The Business Necessity of CS: It's Not an IT Issue'. *Security: Solutions for Enterprise Security Leaders* 51 (3), 56-56

Chan, L., Morgan, I., Simon, H., Alshabanat, F., Ober, D., Gentry, J., Min, D. and Cao, R.. (2019) 'Survey of AI in Cybersecurity for Information Technology Management'. *IEEE Technology & Engineering Management Conference (TEMSCON)*, 1-8

Chander, M., Jain, S. K. and Shankar, R. (2013) 'Modeling of Information Security Management Parameters in Indian Organisations using ISM and MICMAC Approach'. *Journal of Modelling in Management* 8 (2), 171-189

Chang, S. E., Chen, S.-Y. and Chen, C.-Y. (2011) 'Exploring the Relationships between It Capabilities and Information Security Management'. *International Journal of Technology Management*, 54 (2-3), 147-166

Chang, S. E. and Ho, C. B. (2006) 'Organisational Factors to the Effectiveness of Implementing Information Security Management'. *Industrial Management & Data Systems*

Charitoudi, K. and Blyth, A. (2013) 'A Socio-Technical Approach to Cyber Risk Management and Impact Assessment'. *Journal of Information Security* 4 (01), 33

Chatterjee, S., Sarker, S. and Valacich, J. S. (2015) 'The Behavioral Roots of Information Systems Security: Exploring Key Factors Related to Unethical It Use'. *Journal of Management Information Systems*, 31 (4), 49-87

Chatterjee, D. (2019) *Should Executives Go to Jail Over CS Breaches?*. Mahwah, NJ

Chen, L. (2010) 'Businessâ€“It Alignment Maturity of Companies in China'. *Information & Management*, 47 (1), 9-16

Chen, J. and Duvall, G. (eds.) (2014) *9th International Conference on Cyber Warfare and Security 2014, ICCWS 2014*. 'CS Strategy: An Ingredient for Success': Academic Conferences Limited

Cheng, L., Li, Y., Li, W., Holm, E. and Zhai, Q. (2013) 'Understanding the Violation of Is Security Policy in Organisations: An Integrated Model-Based on Social Control and Deterrence Theory'. *Computers & Security*, 39 447-459

Chen, S. P. and Mykletun, R. J. (2014) 'Ageing Workforce Knowledge Management and Transactional & Transformational Leadership'. *International Journal of Business and Social Science* 5 (1)

Chew, E., Swanson, M. M., Stine, K. M., Bartol, N., Brown, A. and Robinson, W. (2008) *Performance Measurement Guide for Information Security*.

Chilisa, B. and Kawulich, B. (2012) 'Selecting a Research Approach: Paradigm, Methodology and Methods'. *Doing Social Research, A Global Context. London: McGraw Hill*

Choo, K. R. (2011) *The Cyber Threat Landscape: Challenges and Future Research Directions* [online]. Available from http://www.sciencedirect.com/science/article/pii/S0167404811001040

Choobineh, J., Dhillon, G., Grimaila, M. R. and Rees, J. (2007) 'Management of Information Security: Challenges and Research Directions'. *Communications of the Association for Information Systems*, 20 (1), 57

Choudrie, J., Zamani, E., Umeoji, E. and Emmanuel, A. (2017) 'Implementing E-Services in Lagos State, Nigeria: The Interplay of Cultural Perceptions and Working Practices During an Automation Initiative: Nigeria E-Government Culture and Working Practices'. *government information quarterly*

Chrapavy, P. (2016) 'Cyber Security Risks: Are they Inflated?'. *Salus Journal* 4 (2), 19

Christ, M. H., Masli, A., Sharp, N. Y. and Wood, D. A. (2015) 'Rotational Internal Audit Programs and Financial Reporting Quality: Do Compensating Controls Help?'. *Accounting, Organisations and Society*, 44 37-59

Cîrnu, C. E., Rotună, C. I., Vevera, A. V. and Boncea, R. (2018) 'Measures to Mitigate Cyber Security Risks and Vulnerabilities in Service-Oriented Architecture'. *Studies in Informatics and Control* 27 (3), 359-368

Cohen, L. 1. a. and Cohen, L.,1928- author (2018) *Research Methods in Education*. Eighth edition / Louis Cohen, Lawrence Manion and Keith Morrison. edn. London: London: Routledge

Coiera, E. (2007) 'Putting the Technical Back into Socio-Technical Systems Research'. *International journal of medical informatics*, 76 S98-S103

Coles-Kemp, L. (2009) 'Information Security Management: An Entangled Research Challenge'. *Information Security Technical Report* 14 (4), 181-185

Colicchia, C., Creazza, A. and Menachof, D. A. (2019) 'Managing Cyber and Information Risks in Supply Chains: Insights from an Exploratory Analysis'. *Supply Chain Management: An International Journal*

Collier, Z. A., DiMase, D., Walters, S., Tehranipoor, M. M., Lambert, J. H. and Linkov, I. (2014) 'CS Standards: Managing Risk and Creating Resilience'. *Computer*, 47 (9), 70-76

Collis, J. and Hussey, R. (2013) *Business Research: A Practical Guide for Undergraduate and Postgraduate Students*.: Palgrave Macmillan

Coltman, T., Tallon, P., Sharma, R. and Queiroz, M. (2015) 'Strategic It Alignment: Twenty-Five Years On'. *Journal of Information Technology*, 30 91-100

Craigen, D., Diakun-Thibault, N. and Purse, R. (2014) 'Defining CS'. *Technology Innovation Management Review*, 4 (10), 13-21

Creswell, J. W. (2013) *Qualitative Inquiry & Research Design: Choosing among Five Approaches*. Third edition. Edn. Los Angeles: SAGE

Creswell, J. W. (2018) *Qualitative Inquiry & Research Design: Choosing among Five Approaches*. Fourth edition / John W. Creswell, Cheryl N. Poth..; International student edition.. edn. Los Angeles: SAGE

Creswell, J. W. and Creswell, J. D. (2017) *Research Design: Qualitative, Quantitative and Mixed Methods Approaches*: Sage publications

Creswell, J. W. and Poth, C. N. (2016) *Qualitative Inquiry and Research Design: Choosing among Five Approaches*. Sage publications

Creswell, J. W. (2007) 'Philosophical, Paradigm and Interpretive Frameworks'. *Qualitative Inquiry and Research Design. Choosing among Five Approaches*, 15-33

Crossan, F. (2003) 'Research Philosophy: Towards an Understanding'. *Nurse Researcher (through 2013)* 11 (1), 46

Crotty, M. (1998) *Foundations of Social Research: Meaning and Perspective in the Research Process*. London: London: SAGE

Culot, G., Fattori, F., Podrecca, M. and Sartor, M. (2019) 'Addressing Industry 4.0 Cybersecurity Challenges'. *IEEE Engineering Management Review*, 47 (3), 79-86

Dalal, R. S., Howard, D. J., Bennett, R. J., Posey, C., Zaccaro, S. J. and Brummel, B. J. (2021) 'Organizational Science and Cybersecurity: Abundant Opportunities for Research at the Interface'. *Journal of Business and Psychology*, 1-29

Dasso, A., Funes, A., Montejano, G., Riesco, D., Uzal, R. and Debnath, N. (2016) 'Model-Based Evaluation of CS Implementations.' in *Information Technology: New Generations*. ed. by Springer, 303-313

Davis, M. C., Challenger, R., Jayewardene, D. N. and Clegg, C. W. (2014) 'Advancing Socio-Technical Systems Thinking: A Call for Bravery'. *Applied Ergonomics* 45 (2), 171-180

Dawson, J. and Thomson, R. (2018) 'The Future CS Workforce: Going Beyond Technical Skills for Successful Cyber Performance'. *Frontiers in psychology*, 9 744

De Bakker, K., Boonstra, A. and Wortmann, H. (2010) *Does Risk Management Contribute to IT Project Success? A Meta-Analysis of Empirical Evidence* [online]. Available from <http://www.sciencedirect.com/science/article/pii/S0263786309000787>

De Bruin, R. and Von Solms, S.H. (2016) 'Cybersecurity Governance: How can we measure it?. ' In *2016 IST-Africa Week Conference*. IEEE, 1-9

DeLone, W. H. and McLean, E. R. (1992) 'Information Systems Success: The Quest for the Dependent Variable'. *Information Systems Research* 3 (1), 60-95

Delone, W. H. and McLean, E. R. (2003) 'The Delone and Mclean Model of Information Systems Success: A Ten-Year Update'. *Journal of Management Information Systems*, 19 (4), 9-30

Denzin, N. K. and Lincoln, Y. S. (2011) *The Sage Handbook of Qualitative Research*.: Sage

Denzin, N. K. and Lincoln, Y. S. (2012) *Collecting and Interpreting Qualitative Materials*.: Sage Publications

Dhillon, G. and Backhouse, J. (2001) 'Current Directions in IS Security Research: Towards Socio-Organisational Perspectives'. *Information Systems Journal*, 11 (2), 127-153

Dhillon, G., Tejay, G. and Hong, W. (2007) 'Identifying Governance Dimensions to Evaluate Information Systems Security in Organisations' in (ed.) *2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07)*. held at IEEE, 157b-157b

Diesch, R., Pfaff, M. and Krcmar, H. (2020) 'A Comprehensive Model of Information Security Factors for Decision-Makers'. *Computers & Security*, 92 101747

Dionne, G. (2013) 'Risk Management: History, Definition and Critique'. *Risk Management and Insurance Review* 16 (2), 147-166

Disparte, D. and Furlow, C. (2017) 'The Best CS Investment You Can Make Is Better Training'. *Harvard business review*, 2-4

Disterer, G. (2013) 'ISO/IEC 27000, 27001 and 27002 for Information Security Management'. *Journal of Information Security*, 4 (02), 92

Doody, O. and Doody, C. M. (2015) 'Conducting a Pilot Study: Case Study of a Novice Researcher'. *British Journal of Nursing*, 24 (21), 1074-1078

Doyle, C. (ed.) (2012) 'Stealing Trade Secrets and Economic Espionage: An Overview of 18 USC 1831 and 1832': Congressional Research Service, Library of Congress

Drack, M. and Schwarz, G. (2010) 'Recent Developments in General System Theory'. *Systems Research and Behavioral Science* 27 (6), 601-610

Dubois, É., Heymans, P., Mayer, N. and Matulevičius, R. (2010) 'A Systematic Approach to Define the Domain of Information System Security Risk Management'. in *Intentional Perspectives on Information Systems Engineering*. ed. by Anon: Springer, 289-306

Dunkerley, K. D. and Tejay, G. (2011) 'A Confirmatory Analysis of Information Systems Security Success Factors'. in (ed.) *2011 44th Hawaii International Conference on System Sciences*. held at IEEE, 1-10

Dugguh, S. I. and Diggi, J. (2015) 'Risk Management Strategies in Financial Institutions in Nigeria: The Experience of Commercial Banks'. *International Journal of Research*, 66

Dzazali, S. and Hussein Zolait, A. (2012) 'Assessment of Information Security Maturity: An Exploration Study of Malaysian Public Service Organisations'. *Journal of Systems and Information Technology*, 14 (1), 23-57

Edwards-Jones, A. (2014) *Qualitative Data Analysis with NVIVO*

Effiok, S., Effiong, C. and Usoro, A. (2012) 'Corporate Governance, Corporate Strategy and Corporate Performance: Evidence from the Financial Institutions Listed on the Nigerian Stock Exchange'. *European Journal of Business and Management*, 4 (18)

Ege, M. S. (2015) *Does Internal Audit Function Quality Deter Management Misconduct?*: American Accounting Association

Egelman, S. and Peer, E. (eds.) (2015) *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*. 'Scaling the Security Wall: Developing a Security Behavior Intentions Scale (Sebis)': ACM

Eisenhardt, K. M. (1989) 'Building Theories from Case Study Research'. *Academy of Management Review* 14 (4), 532-550

Ekelund, S. and Iskoujina, Z. (2019) 'Cybersecurity Economics–Balancing Operational Security Spending'. *Information Technology & People*

Elo, S., Kääriäinen, M., Kanste, O., Pölkki, T., Utriainen, K. and Kyngäs, H. (2014) 'Qualitative Content Analysis: A Focus on Trustworthiness'. *Sage Open* 4 (1)

Evans, L. (2016) 'Protecting Information Assets using ISO/IEC Security Standards'. *Information Management* 50 (6), 28

Falola, T., Genova, A. and Heaton, M. M. (2018) *Historical Dictionary of Nigeria*. Rowman & Littlefield

Feagin, J. R., Orum, A. M. and Sjoberg, G. (1991) *A Case for the Case Study*.: UNC Press Books

Fenz, S., Heurix, J., Neubauer, T. and Pechstein, F. (2014) 'Current Challenges in Information Security Risk Management'. *Information Management & Computer Security*, 22 (5), 410-430

Flick, U. (2018) 'Triangulation in Data Collection'. *The SAGE handbook of qualitative data collection*, 527-544

Flowerday, S. V. and Tuyikeze, T. (2016) 'Information Security Policy Development and Implementation: The What, How and Who'. *Computers & Security*, 61 169-183

Fortune, J. and White, D. (2006) 'Framing of Project Critical Success Factors by a Systems Model'. *International Journal of Project Management*, 24 (1), 53-65

Frank, I. and Odunayo, E. (2013) 'Approach to CS Issues in Nigeria: Challenges and Solution'. *International Journal of cognitive research in science, engineering, and education*, 1 (1)

Fraser, J. R. S. (2016) 'The Role of the Board in Risk Management Oversight'. *The Handbook of Board Governance: A Comprehensive Guide for Public, Private and Not-for-Profit Board Members*, 283

Fielding, J. J. C. F. and Security (2020) 'The People Problem: How CS's Weakest Link Can Become a Formidable Asset'. *Computer Fraud & Security*, 2020 (1), 6-9

Flowerday, S. V. and Tuyikeze, T. (2016) 'Information Security Policy Development and Implementation: The what, how and who'. *Computers & Security* 61, 169-183

Fujs, D., Mihelič, A. and Vrhovec, S.L. (2019) 'The power of interpretation: Qualitative methods in cybersecurity research'. In *Proceedings of the 14th International Conference on Availability, Reliability and Security*,1-10

Galliers, R. D. (1985) 'A1 in Search of a Paradigm for Information Systems Research'

Gana, N. N., Shafi'i, M. A. and Ojeniyi, J. A. (2019) 'Security Risk Analysis and Management in Banking Sector: A Case Study of a Selected Commercial Bank in Nigeria'. *International Journal of Information Engineering and Electronic Business* 11 (2), 35

Ganin, A. A., Quach, P., Panwar, M., Collier, Z. A., Keisler, J. M., Marchese, D. and Linkov, I. (2020) 'Multicriteria Decision Framework for Cybersecurity Risk Assessment and Management'. *Risk Analysis*, 40 (1), 183-199

Gantz, S. D. and Philpott, D. R. (2013) 'Chapter 3 - Thinking About Risk.' in *Fisma and the Risk Management Framework*. ed. by Gantz, S. D. and Philpott, D. R. Syngress, 53-78

Geertz, C. (2004) 'Blurred Genres: The Refiguration of Social Thought'. *The performance studies reader*, 64

Geertz, C. (1980) 'Blurred Genres: The Refiguration of Social Thought'. *The American Scholar*, 165-179

Gehem, M., Usanov, A., Frinking, E. and Rademaker, M. (2015) *Assessing CS: A Meta-Analysis of Threats, Trends and Responses to Cyber Attacks.*: The Hague Centre for Strategic Studies

Gerow, J. E., Grover, V., Thatcher, J. and Roth, P. L. (2014) 'Looking toward the Future of Itâ€“Business Strategic Alignment through the Past'. *MIS Quarterly*, 38 (4), 1159-1186

Gibbs, G., 1948- (2002) *Qualitative Data Analysis: Explorations with NVivo*. Buckingham: Buckingham: Open University Press

Gillam, A. R. and Foster, W. T. J. C. i. H. B. (2020) 'Factors Affecting Risky CS Behaviors by Us Workers: An Exploratory Study'. 106319

Gjerdrum, D. and Peter, M. (2011) 'The New International Standard on the Practice of Risk management–A Comparison of ISO 31000: 2009 and the COSO ERM Framework'. *Risk Management* 31 (2), 8-13

Goni, I. (2019) 'Cyber Security and Computational Laws in Nigerian Banking System'. *Advances in Networks*, 7 (2), 16

Gordon, L. A., Loeb, M. P., Lucyshyn, W. and Zhou, L. (2015) 'The Impact of Information Sharing on CS Underinvestment: A Real Options Perspective'. *Journal of Accounting and Public Policy*, 34 (5), 509-519

Gordon, L. A., Loeb, M. P. and Zhou, L. (2016) 'Investing in CS: Insights from the Gordon-Loeb Model'. *Journal of Information Security*, 7 (02), 49

Goss, D. D. (2017) 'Operationalizing CS — Framing Efforts to Secure U.S. Information Systems'. *The Cyber Defense Review*, 2 (2), 91-110

Gourisetti, S. N. G., Mylrea, M. and Patangia, H. (2020) 'CS Vulnerability Mitigation Framework through Empirical Paradigm: Enhanced Prioritized Gap Analysis'. *Future Generation Computer Systems*, 105 410-431

Greenwood, D. and Sommerville, I. (2011) 'Responsibility Modeling for the Sociotechnical Risk Analysis of Coalitions of Systems'. in (ed.) *Conference Proceedings - IEEE International Conference on Systems, Man and Cybernetics*. held at 1256-1261

Gregor, S. (2006) 'The Nature of Theory in Information Systems'. *MIS Quarterly*, 611-642

Guba, E. G. and Lincoln, Y. S. (1994) 'Competing Paradigms in Qualitative Research'. *Handbook of Qualitative Research* 2 (163-194), 105

Haapamäki, E. and Sihvonen, J. (2019) 'Cyber Security in Accounting Research'. *Managerial Auditing Journal*

Hadlington, L. (2017) Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity and risky cybersecurity behaviours. *Heliyon*, 3(7), p.e00346.

Hagigi, M. and Sivakumar, K. (2009) 'Managing Diverse Risks: An Integrative Framework'. *Journal of International Management* 15 (3), 286-295

Haimes, Y. Y. (2009) 'On the Complex Definition of Risk: A systems-based Approach'. *Risk Analysis* 29 (12), 1647-1654

Hair, J., Joseph F. (2015) *Essentials of Business Research Methods*. 2nd edn

Hampton, J. (2006) 'Risk Pro Knows Value of Networking'. *Business insurance*, 40 (45), 50-50

Harrison, S. and Jürjens, J. (2017) 'Information Security Management and the Human Aspect in Organisations'. *Information and Computer Security*, 25 (5), 494-534

Hart, C. (2018) *Doing a Literature Review: Releasing the Research Imagination*. Sage

Herath, T., Herath, H. and Bremser, W. G. (2010) 'Balanced Scorecard Implementation of Security Strategies: A Framework for IT Security Performance Management'. *Information Systems Management* 27 (1), 72-81

Hinchliffe, A. (2017) 'Nigerian Princes to Kings of Malware: The Next Evolution in Nigerian Cybercrime'. *Computer Fraud & Security*, 2017 (5), 5-9

Hoffman, B. (2006). *Inside Terrorism*.: Columbia University Press

Hoffmann, R., Kiedrowicz, M. and Stanik, J. (eds.) (2016) *MATEC Web of Conferences*. 'Risk Management System as the Basic Paradigm of the Information Security Management System in an Organisation': EDP Sciences

Holliday, A. (2007) *Doing & Writing Qualitative Research*. Sage

Holloway, I. and Biley, F. C. (2011) 'Being a Qualitative Researcher'. *Qualitative Health Research* 21 (7), 968-975

Hopkin, P. (2017) *Fundamentals of Risk Management: Understanding, Evaluating and Implementing Effective Risk Management*. Kogan Page Publishers

Hoyt, R. E. and Liebenberg, A. P. (2011) 'The Value of Enterprise Risk Management'. *Journal of Risk and Insurance*, 78 (4), 795-822

Hu, Q., Dinev, T., Hart, P. and Cooke, D. (2012) *Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organisational Culture**. Atlanta, GA:

Hu, T., Wang, K., Chih, W., and Yang, X. (2020) 'Trade Off Cybersecurity Concerns for Co-Created Value'. *Journal of Computer Information Systems* 60 (5), 468-483

Hubbard, D. W. and Seiersen, R. (2016) *How to Measure Anything in CS Risk*.: John Wiley & Sons

Hudin, N. S. and Hamid, A. B. A. (2014) 'Drivers to the Implementation of Risk Management Practices: A Conceptual Framework'. *Journal of Advanced Management Science*, 2 (3), 163-169

Hull (2015) *Risk Management and Financial Institutions*. 4th edn. Hoboken: Hoboken: Wiley

Hussain, A. and Skinner, G. (2019) 'Reviewing Cyber Security Social Engineering Training and Awareness Programs—Pitfalls and Ongoing Issues'. *Future Internet*, 11 (3), n/a

Ifinedo, P. (2012) 'Understanding Information Systems Security Policy Compliance: An Integration of the Theory of Planned Behavior and the Protection Motivation Theory'. *Computers & Security* 31 (1), 83-95

Ilmudeen, A., Bao, Y. and Alharbi, I. M. (2019) 'How Does Business-It Strategic Alignment Dimension Impact on Organisational Performance Measures'. *Journal of Enterprise Information Management*

Institute of Internal Auditors (2013) 'The Three Lines of Defense in Effective Risk Management and Control'. *Position paper*

Ionita, D. (2013) 'Current Established Risk Assessment Methodologies and Tools'.

Irwin L. (2021) [online] available from<https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-february-2021-2-3-billion-records-breached.html> [15 April 2021]

Islam, M. S., Farah, N. and Stafford, T. F. (2018) 'Factors Associated with Security/Cyber Security Audit by Internal Audit Function: An International Study'. *Managerial Auditing Journal*, 33 (4), 377-409

ISO, I. (2009) 'Risk management–Principles and Guidelines'. International Organisation for Standardization, Geneva, Switzerland

ITU (2022) [online]available from< https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E/> [05 March 2022]

Jackson, M. C. (2007) *Systems Approaches to Management*.: Springer Science & Business Media

Jackson, K. and Bazeley, P. (2019) Qualitative Data Analysis with Nvivo. SAGE Publications Limited

Jankowicz, A. D. (2013) *Business Research Projects* [online]: Springer

Jang-Jaccard, J. and Nepal, S. (2014) 'A Survey of Emerging Threats in Cyber Security'. *Journal of Computer and System Sciences* 80 (5), 973-993

Jarjoui, S. and Murimi, R. (2021) 'A Framework for Enterprise Cybersecurity Risk Management'. in *Advances in Cybersecurity Management*. Springer, 139-161

Javani, B. and Rwelamila, P. M. D. (2016) 'Risk Management in IT Projects–a Case of the South African Public Sector'. *International Journal of Managing Projects in Business*

Jean-Jules, J. and Vicente, R. (2020) 'Rethinking the Implementation of Enterprise Risk Management (Erm) as a Socio-Technical Challenge'. *Journal of Risk Research*, 1-20

Jung, P. W. (2011) 'A Critical Analysis on the Concept of Cyber Security'. *Yonsei Journal of Medical and Science Technology Law* 2 (2), 1-25

Kabanda, S., Tanner, M. and Kent, C. (2018) 'Exploring SME Cybersecurity Practices in Developing Countries'. *Journal of Organizational Computing and Electronic Commerce*, 28 (3), 269-282

Kahyaoglu, S. B. and Caliyurt, K. (2018) 'Cyber Security Assurance Process from the Internal Audit Perspective'. *Managerial Auditing Journal*, 33 (4), 360-376

Kamal, M. M., Bigdeli, A. Z., Themistocleous, M. and Morabito, V. (2015) 'Investigating Factors Influencing Local Government Decision Makers While Adopting Integration Technologies (Inttech)'. *Information & Management*, 52 (2), 135-150

Kaplan, B. and Maxwell, J. A. (2005) 'Qualitative Research Methods for Evaluating Computer Information Systems'. *in Evaluating the Organizational Impact of Healthcare Information Systems*. ed. by Anon: Springer, 30-55

Karpovsky, A. and Galliers, R. D. (2015) 'Aligning in Practice: From Current Cases to a New Agenda'. *Journal of Information Technology*, 30 (2), 136-160

Kayworth, T. and Whitten, D. (2010) 'Effective Information Security Requires a Balance of Social and Technology Factors'. *MIS Quarterly Executive*, 9 (3), 2012-2052

Kendrick, R. (2010) *Cyber Risks for Business Professionals A Management Guide*. Ely: Ely: IT Governance Publishing

Kennedy, S. E. (2016) 'The Pathway to Security-Mitigating User Negligence'. *Information and Computer Security* 24 (3), 255-264

Kerstin, D., Simone, O. and Nicole, Z. (2014) 'Challenges in Implementing Enterprise Risk Management'. *ACRN Journal of Finance and Risk Perspectives* 3 (3), 1-14

Kikwasi, G. (2018) 'Critical Success Factors for Effective Risk Management'. in *Risk Management Treatise for Engineering Practitioners*. ed. by Anon: IntechOpen

Kim, W., Jeong, O., Kim, C., and So, J. (2011) 'The Dark Side of the Internet: Attacks, Costs and Responses'. *Information Systems* 36 (3), 675-705

Kisling, E. L. (2006) *An Implementation of Information Technological Change: A Socio-Technical Systems Methodology Perspective at the Black Chemical Company*

Klein, H. K. and Myers, M. D. (1999) 'A Set of Principles for Conducting and Evaluating Interpretive Field Studies in Information Systems'. *MIS Quarterly*, 67-93

Knight, M. A. (2006) 'A New Era of Development: The Changing Role and Responsibility of Business in Developing Countries'. *Corporate Governance: The International Journal of Business in Society* 12 (4), 403-456

Kosub, T. (2015) 'Components and Challenges of Integrated Cyber Risk Management'. *Zeitschrift fur die gesamte Versicherungswissenschaft*, 104 (5), 615-634

Kotulic, A. G. (2001) *The Security of the IT Resource and Management Support: Security Risk Management Program Effectiveness*. [online] PhD thesis or thesis. United States -- Texas: The University of Texas at Arlington

Kouns, J. and Minoli, D. (2011) Information Technology Risk Management in Enterprise Environments: A Review of Industry Practices and a Practical Guide to Risk Management Teams.: John Wiley & Sons

Kraemer, S., Carayon, P. and Clem, J. (2009) 'Human and Organisational Factors in Computer and Information Security: Pathways to Vulnerabilities'. *Computers & Security*, 28 (7), 509-520
Kumar, S., Biswas, B., Bhatia, M. S. and Dora, M. (2020) 'Antecedents for Enhanced Level of Cyber-Security in Organisations'. *Journal of Enterprise Information Management*

Labaree, R. (2020) 'Organizing Your Social Sciences Research Paper: Theoretical Framework'. 01 November. *USC Libraries, University of Southern California.* [online]. available from < https://libguides.usc.edu/writingguide/theoreticalframework> [27 November 2020]

Lalonde, C. and Boiral, O. (2012) 'Managing Risks through ISO 31000: A Critical Analysis'. *Risk Management* 14 (4), 272-300

Lamidi, M. T. (2020) 'Investigating Cybercrime in Nigeria.' in *Encyclopedia of Criminal Activities and the Deep Web*. ed. by IGI Global, 1018-1033

Lee, I. (2020) 'Internet of Things (IoT) Cybersecurity: Literature Review and IoT Cyber Risk Management'. *Future Internet* 12 (9), 157

Lee, L. S. and Green, E. (2015) 'Systems Thinking and Its Implications in Enterprise Risk Management'. *Journal of Information Systems*, 29 (2), 195-210

Lee, W., Fan, W., Miller, M., Stolfo, S. J. and Zadok, E. (2002) 'Toward Cost-Sensitive Modeling for Intrusion Detection and Response'. *Journal of Computer Security* 10 (1-2), 5-22

Lee, B., and Saunders, M.N. (2017) *Conducting Case Study Research for Business and Management Students*. Los Angeles: Los Angeles: SAGE

Leedy, P. D. and Ormrod, J. E. (2019) 'Practical Research: Planning and Design'. *Pearson*

Leitch, M. (2010) 'ISO 31000: 2009-the New International Standard on Risk Management'. *Risk Analysis* 30 (6), 887

Lewis, S. (2015) 'Qualitative Inquiry and Research Design: Choosing among Five Approaches'. *Health Promotion Practice* 16 (4), 473-475

Li, Y., Dai, W., Bai, J., Gan, X., Wang, J. and Wang, X. (2019) 'An Intelligence-Driven Security-Aware Defense Mechanism for Advanced Persistent Threats'. *IEEE Transactions on Information Forensics and Security*, 14 (3), 646-661

Liang, X. and Xiao, Y. (2013) 'Game Theory for Network Security'. *IEEE Communications Surveys & Tutorials* 15 (1), 472-486

Lin, S., Pizzini, M., Vargus, M. and Bardhan, I. R. (2011) 'The Role of the Internal Audit Function in the Disclosure of Material Weaknesses'. *The Accounting Review*, 86 (1), 287-323

Lincoln, Y. and Guba, E. (1985) 'Thousand Oaks'. *Naturalistic Inquiry*, 290-296

Lincoln, Y. S. and Guba, E. G. (1986) 'But Is It Rigorous? Trustworthiness and Authenticity in Naturalistic Evaluation'. *New directions for program evaluation*, 1986 (30), 73-84

Lund, C. (2014) 'Of what is this a Case? Analytical Movements in Qualitative Social Science Research'. *Human Organisation* 73 (3), 224-234

Lyytinen, K., Mathiassen, L. and Ropponen, J. (1996) 'A Framework for Software Risk Management'. *Journal of Information Technology*, 11 (4), 275-285

Lyytinen, K., Mathiassen, L. and Ropponen, J. (1998) 'Attention Shaping and Software Risk—a Categorical Analysis of Four Classical Risk Management Approaches'. *Information Systems Research*, 9 (3), 233-255

Lyytinen, K. and Newman, M. (2008) 'Explaining Information Systems Change: A Punctuated Socio-Technical Change Model'. *European Journal of Information Systems*, 17 (6), 589-613

Ma, Q., Johnston, A. C. and Pearson, J. M. (2008) 'Information Security Management Objectives and Practices: A Parsimonious Framework'. *Information Management & Computer Security*

Maarop, N., Mustapha, N. M., Yusoff, R., Ibrahim, R. and Zainuddin, N. M. M. (2015) 'Understanding Success Factors of an Information Security Management System Plan Phase Self-Implementation'. *World Academy of Science, Engineering and Technology, International Journal of Social, Behavioral, Educational, Economic, Business and Industrial Engineering*, 9 (3), 884-889

Mackenzie, N. and Knipe, S. (2006) 'Research Dilemmas: Paradigms, Methods and Methodology'. *Issues in Educational Research* 16 (2), 193-205

Maennel, K., Mäses, S., and Maennel, O. (eds.) (2018) *Nordic Conference on Secure IT Systems*. 'Cyber Hygiene: The Big Picture': Springer

Magnusson, E. and Marecek, J. (2015) *Doing Interview-Based Qualitative Research: A Learner's Guide*.: Cambridge University Press

Maisey, M. (2014) 'Moving to Analysis-Led Cyber-Security'. *Network Security*, 2014 (5), 5-12

Makeri, Y. A. (2017) 'Cyber Security Issues in Nigeria and Challenges'. *International Journal*, 7 (4)

Malatji, M., Marnewick, A., and von Solms, S. (2020) 'Validation of a Socio-Technical Management Process for Optimising Cybersecurity Practices'. *Computers & Security* 95, 101846

Malterud, K., Siersma, V. D. and Guassora, A. D. (2016) 'Sample Size in Qualitative Interview Studies: Guided by Information Power'. *Qualitative health research*, 26 (13), 1753-1760

Magnusson, E. and Marecek, J. (2015) *Doing Interview-Based Qualitative Research: A Learner's Guide*.: Cambridge University Press

Manab, N. A., Kassim, I. and Husain, M. R. (2010) 'Enterprise-Wide Risk Management (ERM) Practices: Between Corporate Governance Compliance and Value'. *International Review of Business Research Papers*, 6 (2), 239-252

Marble, R. P. (2000) 'Operationalising the Implementation Puzzle: An Argument for Eclecticism in Research and in Practice'. *European Journal of Information Systems*, 9 (3), 132-147

Martin, C., Bulkan, A. and Klempt, P. (2011) 'Security Excellence from a Total Quality Management Approach'. *Total Quality Management*, 22 (3), 345-371

Masike, M., Sune Von, S. and Marnewick, A. (2019) 'Socio-Technical Systems Cyber Security Framework'. *Information and Computer Security*, 27 (2), 233-272

Masky, M., Young, S. S. and Choe, T. (eds.) (2015) *Information Science and Security (ICISS), 2015 2nd International Conference on*. 'A Novel Risk Identification Framework for Cloud Computing Security': IEEE

Matthews, E. D., Arata, H. J. and Hale, B. L. (2016) 'Cyber Situational Awareness'. *The Cyber Defense Review* 1 (1), 35-46

Maturana, H. R. and Varela, F. J. (2012) *Autopoiesis and Cognition: The Realization of the Living* [online] available from<https://www.google.co.uk/books/edition/Autopoiesis_and_Cognition/iOjVBQAAQBAJ?hl=en&gbpv=1&dq=Maturana+and+Varela+2012&pg=PR11&printsec=frontcover> [28 January 2021]: Springer Science & Business Media

Maurer, C., Kim, K., Kim, D. and Kappelman, L. A. (2021) 'Cybersecurity: Is It Worse Than We Think?'. *Communications of the ACM*, 64 (2), 28-30

Mayer, N. and De Smet, D. (2017) 'Systematic Literature Review and ISO Standards Analysis to Integrate IT Governance and Security Risk Management'

Mazzoccoli, A. and Naldi, M. (2020) 'Robustness of Optimal Investment Decisions in Mixed Insurance/Investment Cyber Risk Management'. *Risk Analysis*, 40 (3), 550-564

McEvoy, T. R. and Kowalski, S. J. (2019) 'Deriving Cyber Security Risks from Human and Organizational Factors–a Socio-Technical Approach'. *Complex Systems Informatics and Modeling Quarterly*, (18), 47-64

McFadzean, E., Ezingeard, J.-N. and Birchall, D. (2006) 'Anchoring Information Security Governance Research: Sociological Groundings and Future Directions'. *Journal of Information System Security*, 2 (3), 3-48

McCurdy, M. (2020) '*The Evolution and Legislative Response to Nigerian Cybercrime* (Doctoral Dissertation, Utica College)

McShane, M., Eling, M. and Nguyen, T. (2021) 'Cyber Risk Management: History and Future Research Directions'. *Risk Management and Insurance Review*

Mena, C., Humphries, A. and Choi, T. Y. (2013) 'Toward a Theory of multi-tier Supply Chain Management'. Journal of Supply Chain Management 49 (2), 58-77

Merete Hagen, J., Albrechtsen, E. and Hovden, J. (2008) 'Implementation and Effectiveness of Organisational Information Security Measures'. *Information Management & Computer Security* 16 (4), 377-397

Meszaros, J. and Buchalcevova, A. (2017) 'Introducing OSSF: A Framework for Online Service CSRM'. *Computers & Security* 65, 300-313

Mikes, A. and Kaplan, R. S. (2014) 'Towards a Contingency Theory of Enterprise Risk Management'.

Miles, M. B., Huberman, A. M., Huberman, M. A. and Huberman, M. (1994) *Qualitative Data Analysis: An Expanded Sourcebook*.: sage

Miller, D., Greenwood, R. and Prakash, R. (2009) 'What Happened to Organization Theory?'. *Journal of Management Inquiry*, 18 (4), 273-279

Minami, N. A., Madnick, S. and Rhodes, D. (eds.) (2008) *American Society for Engineering Management Conference Proceedings, 12-15 November*. 'A Systems Approach to Risk Management'

Mintzberg, H. (1993) *Structure in Fives: Designing Effective Organisations*.: Prentice-Hall, Inc

Mitnick, K. D. and Simon, W. L. (2011) The Art of Deception: Controlling the Human Element of Security. John Wiley & Sons

Morse, E. A. and Raval, V. (2008) 'PCI DSS: Payment Card Industry Data Security Standards in Context'. *Computer Law & Security Review* 24 (6), 540-554

Mukhopadhyay, A., Chatterjee, S., Bagchi, K. K., Kirs, P. J. and Shukla, G. K. (2017) 'Cyber Risk Assessment and Mitigation (CRAM) Framework using Logit and Probit Models for Cyber '. *Information Systems Frontiers*, 1-22

Mumford, E. (2006) 'The Story of socio-technical Design: Reflections on its Successes, Failures and Potential'. *Information Systems Journal* 16 (4), 317-342

Mursu, A. (2002) *Information Systems Development in Developing Countries: Risk Management and Sustainability Analysis in Nigerian Software Companies*.: University of Jyväskylä

Musman, S. and Turner, A. J. (2018) 'A Game Oriented Approach to Minimizing CS Risk'. *International Journal of Safety and Security Engineering* 8 (2), 212-222

Musman, S. and Turner, A. (2018) 'A Game-Theoretic Approach to CSRM'. *The Journal of Defense Modeling and Simulation* 15 (2), 127-146

Myers, M. D. (2013) *Qualitative Research in Business and Management*.: Sage

Myers, M. D. (2019) *Qualitative Research in Business and Management*. Sage Publications Limited

Nastase, P., Nastase, F. and Ionescu, C. (2009) 'Challenges Generated by the Implementation of the IT Standards CobiT 4.1, ITIL v3 and ISO/IEC 27002 in Enterprises'. *Economic Computation & Economic Cybernetics Studies & Research* 43 (3), 1-16

Nather, S. (ed.) (2018) *Proceedings of the 13th International Conference on Cyber Warfare and Security, ICCWS 2018*. 'Improving Information Security through Risk Management and Enterprise Architecture Integration': Academic Conferences and Publishing International Limited

Nazareth, D. L. and Choi, J. (2015) 'A System Dynamics Model for Information Security Management'. *Information & Management* 52 (1), 123-134

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

Neghina, D. and Scarlat, E. (2012) 'Managing Information Technology Security in the Context of Cyber Crime Trends'. *International Journal of Computers Communications & Control* 8 (1), 97-104

Neigel, A. R., Claypoole, V. L., Waldfogle, G. E., Acharya, S., Hancock, G. (2020) 'Holistic Cyber Hygiene Education: Accounting for the Human Factors'. *Computers & Security*, 92, 101731

Neuman, W. L. (2015) *Social Research Methods: Qualitative and Quantitative Approaches*. Seventh edition. edn

Nicho, M. (2018) 'A Process Model for Implementing Information Systems Security Governance'. *Information and Computer Security*, 26 (1), 10-38

Nicho, M., Khan, S. and Rahman, M. (2017) 'Managing Information Security Risk Using Integrated Governance Risk and Compliance'. in (ed.) *Computer and Applications (ICCA), 2017 International Conference on*. held at IEEE, 56-66

Niemimaa, E. and Niemimaa, M. (2017) 'Information Systems Security Policy Implementation in Practice: From Best Practices to Situated Practices'. *European Journal of Information Systems*, 26 (1), 1-20

No, W. G. and Vasarhelyi, M. A. (2017) 'Cyber Security and Continuous Assurance'. *Journal of Emerging Technologies in Accounting*, 14 (1), 1-12

Nwankwo, W. and Ukaoha, K. C. (2019) 'Socio-Technical Perspectives on Cybersecurity: Nigeria's Cybercrime Legislation in Review'. *International Journal of Scientific and Technology Research*, 8 (9), 47-58

Oates, B. J. (2005) *Researching Information Systems and Computing*.: Sage

Office of Government Commerce (2009) *Managing Successful Projects with PRINCE2* [online]: The Stationery Office

Oforji, J. C., Udensi, E. J. and Ibegbu, K. (2017) 'Cyber Security Challenges in Nigeria: The Way Forward'. *Sos Poly Journal of Science & Agriculture, Vol* 2, 2536-2571

Ogoh, P. I. (2016) *The Role Management Plays in Combating Cybercrime within Nigeria's Banking Industry*

O'Gorman, K. D. and MacIntosh, R. (2014) *Research Methods for Business and Management*.: Goodfellow Publishers Limited

Ogu, E. C., Ogu, C. and Oluoha, O. U. (2020) "Global 'Cyber Security Legislation?'-Factors, Perspective and Implications'. *International Journal of Business Continuity and Risk Management*, 10 (1), 80-93

Öğüt, H., Raghunathan, S. and Menon, N. (2011) "Cyber Security Risk Management: Public Policy Implications of Correlated Risk, Imperfect Ability to Prove Loss and Observability of Self-Protection'. *Risk Analysis* 31 (3), 497-512

Okolo, N. B. (2016) Evaluating Factors of Security Policy on Information Security Effectiveness in Developing Nations: A Case of Nigeria: Northcentral University

Olasanmi, O. O. (2019) 'Online Shopping and Customers' Satisfaction in Lagos State, Nigeria'. *American Journal of Industrial and Business Management*, 9 (06), 1446

Olayemi, O. J. (2014) 'A Socio-Technological Analysis of Cybercrime and 'Cyber Security in Nigeria'. *International Journal of Sociology and Anthropology* 6 (3), 116-125

Oliveira, K., Méxas, M., Meiriño, M. and Drumond, G. (2019) 'Critical Success Factors Associated with the Implementation of Enterprise Risk Management'. *Journal of Risk Research*, 22 (8), 1004-1019

Onwubiko, C. (ed.) (2009) International Conference on Global Security, Safety, and Sustainability. 'A Security Audit Framework for Security Management in the Enterprise': Springer

Organ, J. and Stapleton, L. (2012) 'Information Systems Risk through a Socio-Technical Lens: Future Directions in Systems Risk Research'. *IFAC Proceedings Volumes*, 45 (10), 138-143

Orlikowski, W. J. and Baroudi, J. J. (1991) 'Studying Information Technology in Organizations: Research Approaches and Assumptions'. *Information Systems Research*, 2 (1), 1-28

Orlikowski, W. J. (1992) 'The Duality of Technology: Rethinking the Concept of Technology in Organizations'. *Organization Science*, 3 (3), 398-427

Orlikowski, W. J. and Gash, D. C. (1994) 'Technological Frames: Making Sense of Information Technology in Organizations'. *ACM Transactions on Information Systems (TOIS)*, 12 (2), 174-207

Osho, O. and Onoja, A. D. (2015) 'National 'Cyber Security Policy and Strategy of Nigeria: A Qualitative Analysis'. *International Journal of Cyber Criminology*, 9 (1)

Osuagwu, E. U., Chukwudebe, G. A., Salihu, T. and Chukwudebe, V. N. (2015) 'Mitigating Social Engineering for Improved 'Cyber Security'. in (ed.) *2015 International Conference on Cyberspace (CYBER-Abuja)*, held at IEEE, 91-100

Paape, L. and Speklè, R. F. (2012) 'The Adoption and Design of Enterprise Risk Management Practices: An Empirical Study'. *European Accounting Review*, 21 (3), 533-564

Pal, R. (2014) *Improving Network Security through Cyber-Insurance*.: University of Southern California

Palvia, S. C., Sharma, R. S. and Conrath, D. W. (2001) 'A Socio-Technical Framework for Quality Assessment of Computer Information Systems'. *Industrial Management & Data Systems* 101 (5), 237-251

Patton, M. Q. (2015). *Qualitative research & evaluation methods: Integrating theory and practice* (4th ed.). Thousand Oaks, CA: SAGE

Pavlou, P. A. and El Sawy, O. A. (2006) 'From It Leveraging Competence to Competitive Advantage in Turbulent Environments: The Case of New Product Development'. *Information Systems Research*, 17 (3), 198-227

Perez, R. G. (2013) *Effect of organisational factors on information security implementations*

Petter, S., DeLone, W. and McLean, E. (2008) 'Measuring Information Systems Success: Models, Dimensions, Measures and Interrelationships'. *European Journal of Information Systems*, 17 (3), 236-263

Petter, S., DeLone, W. and McLean, E. R. (2013) 'Information Systems Success: The Quest for the Independent Variables'. *Journal of Management Information Systems*, 29 (4), 7-62

Pfleeger, S. L. and Caputo, D. D. (2012) 'Leveraging Behavioral Science to Mitigate 'Cyber Security Risk'. *Computers & Security*, 31 (4), 597-611

Phillips, E. M. and Pugh, D. S. (2010) *How to Get a PhD a Handbook for Students and their Supervisors* [online] 5th edition. edn. Berkshire, England: Berkshire, England: McGraw-Hill: Open University Press

Power, M. (2011) 'Smart and Dumb Questions to Ask About Risk Management'. *Risk watch: thought leadership in risk and governance*, 2-5

Power, M., Ashby, S. and Palermo, T. (2013) *Risk Culture in Financial Organisations: A Research Report*. CARR-Analysis of Risk and Regulation

Project Management Institute (2009) 'Practice Standard for Project Risk Management'. in (ed.) held at Project Management Institute

Puhakainen, P. and Siponen, M. (2010) 'Improving Employees' Compliance through Information Systems Security Training: An Action Research Study'. *MIS Quarterly*, 757-778

Purdy, G. (2011) 'Risk Appetite: Is Using This Concept Worth the Risk'. *New Zealand: Risk Post*

Purdy, G. (2010) 'ISO 31000: 2009—setting a New Standard for Risk Management'. *Risk Analysis* 30 (6), 881-886

Raggad, B. G. (2010) Information Security Management: Concepts and Practice: CRC Press

Rahman, M. A. and Al-Shaer, E. (2013) 'A Formal Approach for Network Security Management Based on Qualitative Risk Analysis'. in (ed.) *2013 IFIP/IEEE International Symposium on Integrated Network Management (IM 2013)*. held at IEEE, 244-251

Ram, J., Corkindale, D. and Wu, M.L. (2013) 'Implementation Critical Success Factors (Csfs) for Erp: Do They Contribute to Implementation Success and Post-Implementation Performance?'. *International Journal of Production Economics*, 144 (1), 157-174

Raz, T., Shenhar, A. J. and Dvir, D. (2002) 'Risk Management, Project Success and Technological Uncertainty'. *R&D Management* 32 (2), 101-109

Reybold, L. E., Lammert, J. D. and Stribling, S. M. (2013) 'Participant Selection as a Conscious Research Method: Thinking Forward and the Deliberation of 'emergent' findings'. *Qualitative Research* 13 (6), 699-716

Reza Hosseini, M., Chileshe, N., Jepson, J. and Arashpour, M. (2016) 'Critical Success Factors for Implementing Risk Management Systems in Developing Countries'. *Construction Economics and Building* 16 (1), 18-32

Rhee, H.-S., Ryu, Y. U. and Kim, C.-T. (2012) 'Unrealistic Optimism on Information Security Management'. *Computers & Security*, 31 (2), 221-232

Rios Insua, D., Couce-Vieira, A., Rubio, J. A., Pieters, W., Labunets, K. and G. Rasines, D. (2021) 'An Adversarial Risk Analysis Framework for Cybersecurity'. *Risk Analysis*, 41 (1), 16-36

Ritchie, J., Lewis, J., Nicholls, C. M. and Ormston, R. (2013) *Qualitative Research Practice: A Guide for Social Science Students and Researchers*.: sage

Rivard, S., Raymond, L. and Verreault, D. (2006) 'Resource-Based View and Competitive Strategy: An Integrated Model of the Contribution of Information Technology to Firm Performance'. *The Journal of Strategic Information Systems*, 15 (1), 29-50

Robertson, M. M., Hettinger, L. J., Waterson, P. E., Ian Noy, Y., Dainoff, M. J., Leveson, N. G., Carayon, P. and Courtney, T. K. (2015) 'Sociotechnical Approaches to Workplace Safety: Research Needs and Opportunities'. *Ergonomics* 58 (4), 650-658

Rockart, J. F. (1979) 'Chief Executives Define Their Own Data Needs'. *Harvard Business Review* 57 (2), 81-93

Rockart, J. F. (1980) 'The Changing Role of the Information Systems Executive: A Critical Success Factors Perspective'

Rogers, P. J. (2000) 'Program Theory: Not Whether Programs Work but how they Work'. in *Evaluation Models*. ed. by Anon: Springer, 209-232

Rothrock, R. A., Kaplan, J. and Van Der Oord, F. (2018) 'The Board's Role in Managing 'Cyber Security Risks'. *MIT Sloan Management Review* 59 (2), 12-15

Rudestam, K. E. and Newton, R. R. (2014) *Surviving Your Dissertation: A Comprehensive Guide to Content and Process* [online]: Sage publications

Ryan, J. J. C. H., Mazzuchi, T. A., Ryan, D. J., Lopez De La Cruz, J. and Cooke, R. (2012) 'Quantifying Information Security Risks using Expert Judgment Elicitation'. *Computers and Operations Research* 39 (4), 774-784
294

Saber, J. A. (2016) *Determining Small Business Cybersecurity Strategies to Prevent Data Breaches*

Sadgrove, K. (2016) *The Complete Guide to Business Risk Management*.: Routledge

Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A. and Herawan, T. (2015) 'Information Security Conscious Care Behaviour Formation in Organisations'. *Computers & Security* 53, 65-78

Safa, N. S., Von Solms, R. and Furnell, S. (2016) 'Information Security Policy Compliance Model in Organisations'. *Computers & Security* 56, 70-82

Salim, H. M. (2014) Cyber Safety: A Systems Thinking and Systems Theory Approach to Managing 'Cyber Security Risks

Saleh, M. S. and Alfantookh, A. (2011) 'A New Comprehensive Framework for Enterprise Information Security Risk Management'. *Applied Computing and Informatics* 9 (2), 107-118

Sallos, M. P., Garcia-Perez, A., Bedford, D. and Orlando, B. (2019) 'Strategy and Organisational Cybersecurity: A Knowledge-Problem Perspective'. *Journal of Intellectual Capital*

Salmi, A. and Mattelmäki, T. (2019) 'From within and in-Between–co-Designing Organizational Change'. *CoDesign*

Sarker, S., Chatterjee, S., Xiao, X., and Elbanna, A. (2019) 'The Sociotechnical Axis of Cohesion for the IS Discipline: Its Historical Legacy and its Continued Relevance'. *Mis Quarterly* 43 (3), 695-720

Saulawa, M. A. and Abubakar, M. (2014) 'Cybercrime in Nigeria: An Overview of Cybercrime Act 2013'. *JL Pol'y & Globalization* 32, 23

Saunders, J. (2017) 'Tackling Cybercrime – the UK Response'. *Journal of Cyber Policy* 2 (1), 4-15

Saunders, M.N.K., Thornhill, A. and Lewis, P. (2016) *Research Methods for Business Students*. Seventh edition. edn

Schatz, D., Bashroush, R. and Wall, J. (2017) 'Towards a More Representative Definition of 'Cyber Security'. *Journal of Digital Forensics, Security and Law* 12 (2), 8

Schiller, F. and Prpich, G. (2014) 'Learning to Organise Risk Management in Organisations: What Future for Enterprise Risk Management?'. *Journal of Risk Research*, 17 (8), 999-1017

Schlosser, F., Beimborn, D., Weitzel, T. and Wagner, H.-T. (2015) 'Achieving Social Alignment between Business and It–an Empirical Evaluation of the Efficacy of It Governance Mechanisms'. *Journal of Information Technology*, 30 (2), 119-135

Scotland, J. (2012) 'Exploring the Philosophical Underpinnings of Research: Relating Ontology and Epistemology to the Methodology and Methods of the Scientific, Interpretive, and Critical Research Paradigms'. *English Language Teaching* 5 (9), 9

Sekaran, U. and Bougie, R. (2016) *Research Methods for Business: A Skill Building Approach*.: John Wiley & Sons

Shackelford, S. J. (2016) 'Business and Cyber Peace: We Need You!'. *Business Horizons* 59 (5), 539-548

Shackelford, Scott J, JD, PHD, Proia, A. A., JD, Martell, B., JD and Craig, Amanda N, MSC, JD (2015) 'Toward a Global 'Cyber Security Standard of Care?: Exploring the Implications of the 2014 NIST CS Framework on Shaping Reasonable National and International CS Practices'. *Texas International Law Journal* 50 (2/3), 305-355

Shah, M. H., Jones, P. and Choudrie, J. (2019) 'Cybercrimes Prevention: Promising Organisational Practices'. *Information Technology & People*

Shamala, P., Ahmad, R., Zolait, A. and Sedek, M. (2017) 'Integrating Information Quality Dimensions into Information Security Risk Management (ISRM)'. *Journal of Information Security and Applications* 36, 1-10

Sharkov, G. (2016) 'From CS to Collaborative Resiliency'. in (ed.) *Proceedings of the 2016 ACM Workshop on Automated Decision Making for Active Cyber Defense*. held at ACM, 3-9

Siccama, C. J. and Penna, S. (2008) 'Enhancing Validity of a Qualitative Dissertation Research Study by using NVivo'. *Qualitative Research Journal* 8 (2), 91-103

Silverman, D. (2017). *Doing Qualitative Research*. Fifth edition. edn

Simon, S. J. (2004) 'Critical Success Factors for Electronic Services: Challenges for Developing Countries'. *Journal of Global Information Technology Management* 7 (2), 31-53

Singh, A. N., Gupta, M. P. and Ojha, A. (2014) 'Identifying Factors of "Organisational Information Security Management'. *Journal of Enterprise Information Management*

Singh, J., Millard, C., Reed, C., Cobbe, J., and Crowcroft, J. (2018) 'Accountability in the IoT: Systems, Law, and Ways Forward'. *Computer* 51 (7), 54-65

Siponen, M. and Willison, R. (2009) 'Information Security Management Standards: Problems and Solutions'. *Information & Management*, 46 (5), 267-270

Siponen, M., Mahmood, M. A. and Pahnila, S. (2014) 'Employees' Adherence to Information Security Policies: An Exploratory Field Study'. *Information & Management*, 51 (2), 217-224

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 and Management* 135 (10), 965-978

Sobers, R. (2020) 107 Must-Know Data Breach Statistics for 2020. 24 September. available from < https://www.varonis.com/blog/data-breach-statistics/#recent> [26 November 2020]

Soomro, Z. A., Shah, M. H. and Ahmed, J. (2016) 'Information Security Management Needs More Holistic Approach: A Literature Review'. *International Journal of Information Management* 36 (2), 215-225

Spagnoletti, P. and Resca, A. (2008) 'The Duality of Information Security Management: Fighting Against Predictable and Unpredictable Threats'. *Journal of Information System Security* 4 (3), 46-62

Spears, J. L. and Barki, H. (2010) 'User Participation in Information Systems Security Risk Management'. *MIS Quarterly*, 503-522

Spremić, M. and Šimunic, A. (2018) 'Cyber security challenges in digital economy'. In *Proceedings of the World Congress on Engineering* (1), 341-346

Srinidhi, B., Yan, J. and Tayi, G. K. (2015) 'Allocation of Resources to Cyber-Security: The Effect of Misalignment of Interest between Managers and Investors'. *Decision Support Systems* 75, 49-62

Srivastava, A. K. (2017) 'Alignment: The Foundation of Effective Strategy Execution'. *International Journal of Productivity and Performance Management*

Stewart, R. W. and Fortune, J. (1995) 'Application of Systems Thinking to the Identification, Avoidance and Prevention of Risk'. *International Journal of Project Management* 13 (5), 279-286

Stewart, H. and Jürjens, J. (2017) 'Information Security Management and the Human Aspect in Organisations'. *Information & Computer Security*, 25 (5), 494-534

Stuart, I., McCutcheon, D., Handfield, R., McLachlin, R. and Samson, D. (2002) 'Effective Case Research in Operations Management: A Process Perspective'. *Journal of Operations Management* 20 (5), 419-433

Symantec Security Response Team (2019) *ISTR 24: Symantec's Annual Threat*. 19 February. available from<https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/istr-24-cyber-security-threat-landscape> [20 August 2019]

Tagarev, T. (2020) 'Towards the Design of a Collaborative Cybersecurity Networked Organisation: Identification and Prioritisation of Governance Needs and Objectives'. *Future Internet* 12 (4), 62

Talbot, J. a. (2009) *Security Risk Management: Body of Knowledge*.

Thomson, K. and von Solms, R. (2006) *Towards an Information Security Competence Maturity Model* [online]. available from <http://www.sciencedirect.com/science/article/pii/S1361372306703566>

Tisdale, S. M. (2016) 'Architecting A Cyber Security Management Framework.'. *Issues in Information Systems* 17 (4)

Tisdale, S. M. (2015) 'Cyber Security: Challenges from a Systems, Complexity, Knowledge Management and Business Intelligence Perspective'. *Issues in Information Systems*, 16 (3)

Toma, S., Chiriţă, M., and Şarpe, D. (2012) 'Risk and Uncertainty'. *Procedia Economics and Finance* 3, 975-980

Toregas, C. and Zahn, N. (2014) 'Insurance for Cyber Attacks: The Issue of Setting Premiums in Context'. *George Washington University*

Torres, J. M., Sarriegi, J. M., Santos, J. and Serrano, N. (2006) 'Managing Information Systems Security: Critical Success Factors and Indicators to Measure Effectiveness'. in (ed.) *International Conference on Information Security*. held at Springer, 530-545

Touhill, G. J. and Touhill, C. J. (2014) *Cyber Security for Executives: A Practical Guide*.: John Wiley & Sons

Transparency report (2020) [online] available from< https://transparencyreport.google.com/safe-browsing/overview>[27 January 2021]

Trim, P. and Lee, Y.-I. (2014) *Cyber Security Management: A Governance, Risk and Compliance Framework*. Gower Publishing, Ltd.

Troyer, L. (2017) 'Expanding Sociotechnical Systems Theory through the Trans-Disciplinary Lens of Complexity Theory.' in *Transdisciplinary Perspectives on Complex Systems*. ed. by Springer, 177-192

Tu, C. Z., Yuan, Y., Archer, N. and Connelly, C. E. (2018) 'Strategic Value Alignment for Information Security Management: A Critical Success Factor Analysis'. *Information & Computer Security*, 26 (2), 150-170

Tu, Z. and Yuan, Y. (2014) 'Critical Success Factors Analysis on Effective Information Security Management: A Literature Review'

Tu, Z. (2016) *Information security management: A critical success factors analysis.* [online] Doctoral thesis, McMaster University, Ontario.

Turel, O., Liu, P. and Bart, C. (2017) 'Board-Level Information Technology Governance Effects on Organisational Performance: The Roles of Strategic Alignment and Authoritarian Governance Style'. *Information Systems Management*, 34 (2), 117-Trim 136

Ulsch, M. (2014) Cyber Threat!: How to Manage the Growing Risk of Cyber Attacks.: John Wiley & Sons

Usman, A. K. M. and Shah, M. H. P. (2013) 'Critical Success Factors for Preventing E-Banking Fraud'. *Journal of Internet Banking and Commerce*, 18 (2), 1-15

Vaismoradi, M., Jones, J., Turunen, H. and Snelgrove, S. (2016) 'Theme Development in Qualitative Content Analysis and Thematic Analysis'. *Journal of Nursing Education and Practice*, 6 (5), 100

Vakharia, A. B., Mishra, V. and Kumar, S. (2012) 'Security Glitches related to e-Commerce and their Solutions'

Van Erp, J. (2017) 'New Governance of Corporate Cyber Security: A Case Study of the Petrochemical Industry in the Port of Rotterdam'. *Crime, Law and Social Change*, 68 (1-2), 75-93

Veiga, A. D. and Eloff, J. H. (2007) 'An Information Security Governance Framework'. *Information systems management*, 24 (4), 361-372

Verkerke, A. T. (2015) 'Towards a Cyber Approach for Large Organisations'.

Vincent, N. E., Higgs, J. L. and Pinsker, R. E. (2017) 'It Governance and the Maturity of It Risk Management Practices'. *Journal of Information Systems*, 31 (1), 59-77

Vishwanath, A., Neo, L. S., Goh, P., Lee, S., Khader, M., Ong, G. and Chin, J. (2020) 'Cyber Hygiene: The Concept, Its Measure and Its Initial Tests'. *Decision Support Systems*, 128, 113160

Von Solms, R. and Van Niekerk, J. (2013) 'From Information Security to Cyber Security'. *Computers & Security*, 38, 97-102

Von Solms, B. and Von Solms, R. (2018) 'Cyber Security and Information Security–What Goes Where?'. *Information & Computer Security*

Vose, D. (2008) *Risk Analysis: A Quantitative Guide*. John Wiley & Sons

Wall, D. (2007) Cybercrime: The Transformation of Crime in the Information Age.: Polity

Wallace, M. and Wray, A. (2021) *Critical Reading and Writing for Postgraduates*. Sage

Walliman, N. (2017) *Research Methods: The Basics*.: Routledge

Walliman, N. (2006) *Social Research Methods*. London: London: SAGE

Walsham, G. (2006) 'Doing Interpretive Research'. *European Journal of Information Systems*, 15 (3), 320-330

Walsham, G. (1995b) 'Interpretive Case Studies in IS Research: Nature and Method'. *European Journal of Information Systems* 4 (2), 74-81

Walsham, G. (1995a) 'The Emergence of Interpretivism in IS Research'. *Information Systems Research* 6 (4), 376-394

Waly, N.S. (2013) *Organisational information security management: The impact of training and awareness. Evaluating the socio-technical impact on organisational information security policy management.* [online] Doctoral thesis, University of Bradford

Wang, E. T. G., Klein, G. and Jiang, J. J. (2006) 'Erp Misfit: Country of Origin and Organisational Factors'. *Journal of Management Information Systems*, 23 (1), 263-292

Wang, N., Xue, Y., Liang, H. and Ge, S. (2011) 'The Road to Business-IT Alignment: A Case Study of Two Chinese Companies'. *CAIS*, 28 26

Wang, V., Nnaji, H. and Jung, J. (2020) 'Internet Banking in Nigeria: Cyber Security Breaches, Practices and Capability'. *International Journal of Law, Crime and Justice*, 62, 100415

Warkentin, M. and Willison, R. (2009) 'Behavioral and Policy Issues in Information Systems Security: The Insider Threat'. *European Journal of Information Systems* 18 (2), 101-105

Webb, J., Ahmad, A., Maynard, S. B. and Shanks, G. (2014) 'A Situation Awareness Model for Information Security Risk Management'. *Computers & Security* 44, 1-15

Weill, P. and Olson, M. H. (1989) 'An Assessment of the Contingency Theory of Management Information Systems'. *Journal of Management Information Systems*, 6 (1), 59-86

Werlinger, R., Hawkey, K. and Beznosov, K. (2009) 'An Integrated View of Human, Organisational and Technological Challenges of It Security Management'. *Information Management & Computer Security*, 17 (1), 4-19

White, A. E. (2014) Threat Assessment of Cyber Attacks on Retail and Financial Organisations

White, C., Woodfield, K. and Ritchie, J. (2003) 'Reporting and Presenting Qualitative Data'. *Qualitative Research Practice: A Guide for Social Science Students and Researchers*, 287-320

White, G. R., Allen, R. A., Samuel, A., Abdullah, A. and Thomas, R. J. (2020) 'Antecedents of Cybersecurity Implementation: A Study of the Cyber-Preparedness of Uk Social Enterprises'. *IEEE Transactions on Engineering Management*

Whitman, M. E. and Mattord, H. J. (2011) *Principles of Information Security*.: Cengage Learning

Williams, J. and Ramaprasad, A. (1996) 'A Taxonomy of Critical Success Factors'. *European Journal of Information Systems*, 5 (4), 250-260

Willison, R. and Siponen, M. (2009) 'Overcoming the Insider: Reducing Employee Computer Crime through Situational Crime Prevention'. *Communications of the ACM* 52 (9), 133-137

Wilson, K., Roe, B. and Wright, L. (1998) *Telephone Or Face-to-Face Interviews?: A Decision made on the Basis of a Pilot Study*

Wray, A. and Wallace, M. (2021) 'Critical Reading and Writing for Postgraduates'. *Critical Reading and Writing for Postgraduates*, 1-320

Wu, S. P.J., Straub, D. W., and Liang, T.P. (2015) 'How Information Technology Governance Mechanisms and Strategic Alignment Influence Organisational Performance: Insights from a Matched Survey of Business and It Managers'. *MIS Quarterly*, 39 (2), 497-518

Yang, L. (2011) 'Study on the Improvement of the Internal Audit Work in It Environment'. in (ed.) *2011 Fourth International Symposium on Knowledge Acquisition and Modeling*. held at IEEE, 233-236

Yaraghi, N. and Langhe, R. G. (2011) 'Critical Success Factors for Risk Management Systems'. *Journal of Risk Research* 14 (5), 551-581

Yasin, M. M., Czuchry, A. J. and Small, M. H. (2018) 'Organizational Security: A Conceptual Framework and Implementation Issues'. *Competition Forum*, 16 (1), 38-49

Yayla, A. A. and Hu, Q. (2012) 'The Impact of It-Business Strategic Alignment on Firm Performance in a Developing Country Setting: Exploring Moderating Roles of Environmental Uncertainty and Strategic Orientation'. *European Journal of Information Systems*, 21 (4), 373-387

Yilmaz, K. (2013) 'Comparison of Quantitative and Qualitative Research Traditions: Epistemological, Theoretical and Methodological Differences'. *European Journal of Education* 48 (2), 311-325

Yin, R. K. (2003) 'Designing Case Studies'. *Qualitative Research Methods*.Sage publications

Yin, R. K. (2013) *Case Study Research: Design and Methods*. Sage publications

Yin, R. K. (2009) 'Case Study Research: Design and Methods Fourth Edition'. *Los Angeles and London: SAGE*

Yin, R. K. (2018) *Case Study Research and Applications: Design and Methods*. Sixth edition. edn.

Yin, R. K. (2014) *Case Study Research: Design and Methods*. Fifth edition. edn. Los Angeles: Los Angeles: SAGE

Young, W. and Leveson, N. G. (2014) 'An Integrated Approach to Safety and Security Based on Systems Theory'. Communications of the ACM, 57 (2), 31-35

Zafar, H., Clark, J. G., Ko, M. S. and Au, Y. A. (2011) 'Critical Success Factors for an Effective Security Risk Management Program: An Exploratory Case Study at a Fortune 500 Firm'. in (ed.) *AMCIS*.

Zammani, M. and Razali, R. (2016) 'An Empirical Study of Information Security Management Success Factors'. *International Journal on Advanced Science, Engineering, and Information Technology* 6 (6), 904-913

Zhao, X., Xue, L. and Whinston, A. B. (2013) 'Managing Interdependent Information Security Risks: Cyber insurance, Managed Security Services and Risk Pooling Arrangements'. *Journal of Management Information Systems*, 30 (1), 123-152

Zoto, E., Kianpour, M., Kowalski, S. J., and Lopez-Rojas, E. A. (2019) 'A Socio-Technical Systems Approach to Design and Support Systems Thinking in Cybersecurity and Risk Management Education'. *Complex Systems Informatics and Modeling Quarterly* (18), 65-75

Zwikael, O. and Ahn, M. (2011) 'The Effectiveness of Risk Management: An Analysis of Project Risk Planning across Industries and Countries'. *Risk Analysis: An International Journal*, 31 (1), 25-37

Appendix A: Letter of Introduction

EVALUATION OF SUCCESS FACTORS FOR CYBERSECURITY RISK MANAGEMENT IN THE LARGE ORGANISATIONS IN NIGERIA

PARTICIPANT INFORMATION SHEET

You are being invited to take part in research to evaluation of success factors of cybersecurity risk management (CSRM) in the large organisations in Nigeria. Olukemi Olaniran, researcher at Coventry University is leading this research. Before you decide to take part, it is important you understand why the research is being conducted and what it will involve. Please take time to read the following information carefully.

What is the purpose of the study?
The purpose of the study is to evaluation of success factors of cybersecurity risk management (CSRM) in large organisations in Nigeria.

Why have I been chosen to take part?
You are invited to participate in this study in order to conduct a credible research, being an individual with relevant experience in the sector and can speak on your behalf and on behalf of the organisation.

What are the benefits of taking part?
By sharing your experiences with us, you will be helping Olukemi Olaniran and Coventry University to evaluation of success factors of cybersecurity risk management (CSRM) in the large organisations in Nigeria. By participating in this research, you will be contributing to practice in improving the success of cyber security risk management implementation in large organisations in Nigeria. A detailed feedback of the analysis of the research comprising the feedback from your organisation and other one or two large organisations will be available to you.

Are there any risks associated with taking part?
This study has been reviewed and approved through Coventry University's formal research ethics procedure. There are no significant risks associated with participation.

Do I have to take part?
No – it is entirely up to you. If you do decide to take part, please keep this Information Sheet, and complete the Informed Consent Form to show that you understand your rights in relation to the research, and that you are happy to participate. Please note down your participant number (which is on the Consent Form) and provide this to the lead researcher if you seek to withdraw from the study at a later date. You are free to withdraw your information from the project data set at any time until the data are destroyed on 31/5/2020. You should note that your data may be used in the production of formal research outputs (e.g. journal articles, conference papers, theses, and reports) prior to this date and so you are advised to contact the university at the earliest opportunity should you wish to withdraw from the study. To withdraw, please contact the lead researcher (contact details are provided below). Please also contact the Research Support Office email researchproservices.fbl@coventry.ac.uk; telephone +44(0)2477658461 so that your request can be dealt with promptly in the event of the lead researcher's absence. You do not need to give a reason. A decision to withdraw, or not to take part, will not affect you in any way.

What will happen if I decide to take part?
You will be asked a number of questions regarding success factors for cybersecurity risk management. The interview will take place via skype at a time that is convenient to you during normal business hours. Ideally, you would not audio record your responses, so the location should be in a fairly quiet area. The interview should complete within an hour.

Data Protection and Confidentiality
Your data will be processed in accordance with the General Data Protection Regulation 2016 (GDPR) and the Data Protection Act 2018. All information collected about you will be kept strictly confidential. Unless they are fully anonymised in our records, your data will be referred to by a unique participant number rather than by name. If you consent to being audio recorded, all recordings will be destroyed once they have been transcribed. Your data will only be viewed by the researcher/research team. All electronic data will be stored on a password-protected computer file in Coventry University One Drive. All paper records will be stored in a locked filing cabinet safely on campus. Your consent information will be kept separately from your responses in order to minimise risk in the event of a data breach. The lead researcher will take responsibility for data destruction and all collected data will be destroyed on or before 31/5/2020.

Data Protection Rights
Coventry University is a Data Controller for the information you provide. You have the right to access information held about you. Your right of access can be exercised in accordance with the General Data Protection Regulation and the Data Protection Act 2018. You also have other rights including rights of correction, erasure, objection, and data portability. For more details, including the right to lodge a complaint with the Information Commissioner's Office, please visit www.ico.org.uk. Questions, comments, and requests about your personal data can also be sent to the University Data Protection Officer - enquiry.ipu@coventry.ac.uk

What will happen with the results of this study?
The results of this study may be summarised in published articles, reports and presentations. Quotes or key findings will always be made anonymous in any formal outputs unless we have your prior and explicit written permission to attribute them to you by name.

Making a Complaint
If you are unhappy with any aspect of this research, please first contact the lead researcher, Olukemi Olaniran, olanira2@uni.coventry.ac.uk or 07587611746. If you still have concerns and wish to make a formal complaint, please write to:

Dr Mahmood shah
Senior Lecturer in e-Business and PhDs Coordinator
Coventry University
Coventry CV1 5DL
Email: ac3559@coventry.ac.uk

In your letter, please provide information about the research project, specify the name of the researcher and detail the nature of your complaint.

Appendix B: Interview Agenda

Question Tags/Interview objective	Main Questions	Sub Question	Source
Part A: Background Question	A1: What is your job function that is related to CSRM? A3: How successful do you feel about the overall implementation of cybersecurity risk management in your organisation?	A2: How many years of experience do you have on the job? A4: How does your organisation measure cybersecurity risk management implementation success?	Al-Awadi and Renaud (2007), Al-Awadi (2009) Tu (2016)
Part B: (RQ 4) Organisational Factors			
Business Alignment	B1: Describe the extent to which you feel that the cybersecurity risk management goals are well-aligned with the rest of the business objectives, value or needs?	B2: Describe how the alignment of the cybersecurity risk management objective with the rest of the business objective has increased your organisational cybersecurity risk management success?	Perez (2013), Spears and Barki (2010), Herath, Herath and Bremser (2010)
Budget/ Investment	B3: How would you describe the impact of top management support on investment/funding on cybersecurity risk management success in your company?	B4: Do you think investment in cybersecurity risk management creates value for the organisation?	Al-Awadi and Renaud (2007), Torres et al. (2006), Tu (2016)
Corporate Governance	B5: How is the cybersecurity risk management governance structure organised in your organisation?	B6: In your opinion, how has the success of cybersecurity risk management been improved through governance?	Allen et al. (2018b), Armstrong et al. (2015), Islam, Farah and Stafford (2018).
Part C: (RQ1) People Factors			
Awareness	C1: In your organisation, what initiatives have your organisation taken to create awareness of CSRM implementation to all stakeholders or employees? Which medium?	C2: In your organisation, how often are awareness education of cyber threats and countermeasures provided to all stakeholders or employees?	Al-Awadi and Renaud (2007), Ani, He and Tiwari (2019), Matthews, Arata and Hale (2016), Tu (2016)

	C3: Explain how your organisation's cybersecurity risk management awareness programme has contributed to strengthening transaction security?	C4: Do you think awareness education has reduced cybersecurity risk management deficiencies in your organisation?	Merete Hagen, Albrechtsen and Hovden (2008), Spears and Barki (2010)
Training	C5: In your organisation, what current programme do you have to train employees/stakeholders about policies, procedures, or countermeasures for cybersecurity risk management?	C6: What mediums are used for training? C7: How has the cybersecurity risk management capability of all stakeholders been beneficial to your organisation?	Al-Awadi (2009), Disparte and Furlow (2017), Kennedy (2016) Waly (2013)
Top Management Support	C8: How you think top management support is critical for the success of cybersecurity risk management implementation? Please explain with examples.	C9: How has top management communicated its active support for cybersecurity risk management success? Please, give examples.	Chatterjee (2019), Tu et al. (2018).
Part D: (RQ 2) Technology Factors			
IT Competence	D1: How has the IT capability of staff, both inbound and outsourced, helped achieve CSRM success in your organisation?	D2:: How you measure end-users of IT systems follow sound CSRM operation processes? Explain.	Tu (2016), Tu et al. (2018).
System quality (Task Technology fit)	D3: What technology tools and techniques have been adopted for CSRM? D5: What impacts have the technology solutions had in protecting the numerous organisational vulnerabilities and endpoints?	D4: What are the types of authentication used for access authentication and transactional authentication?	Palvia, Sharma and Conrath (2001), Petter, DeLone and McLean (2013), Lyytinen and Newman (2008), Usman and Shah (2013).
Part E: (RQ 3) Process Factors (Security Controls)			
Risk Management	E1: In your organisation, what are the risk management procedures/standards/or countermeasures to ensure cybersecurity risk management success?	E2: How effective are these procedures/standards in identifying and reducing cyber threat and attack in your organisation?	Gatzert and Schmit (2016), Herath, Herath and Bremser (2010), Tu et al. (2018)
CSRM Policies	E3: In your organisation, what are the policies to ensure cybersecurity risk management success?	E4: How successful is your organisation at practising cybersecurity risk management policies?	Al-Awadi and Renaud 2007), Al-Awadi (2009), Nather (2018),

	E5: How effective is the implementation of security policies in your organisation in reducing cybersecurity breaches in the last five years?		Tu (2016), Waly (2013)
Part F: Framework Review			
	F1: A literature review on prior research was used to propose a cybersecurity risk management success factors framework (a recap). What is your view on the factors that have been identified?	F2: Has an appropriate grouping of success factors been adopted? F3: Would you like to have a summary of the result of this study by email?	Usman (2018).

Table B1: Summary and Description of Success Factors

Factor	Description
Business alignment	To confirm whether CSRM strategic objectives and controls should align with organisational goals to achieve CSRM success
Top management support	To substantiate whether top management's total commitment and strong leadership are necessary to achieve CSRM outcome.
Budget planning	To confirm the importance of the budget planning process to support and carry out CSRM activities. Budget planning includes financial and human resources.
Risk management	To reveal the importance of risk management phases and clear procedures (identification, assessment, communication and treatment) to either eliminate or reduce CS risks to a reasonable level documented in standards/framework is key to the success of CSRM implementation.
CSRM policies	To confirm that CSRM policies are comprehensive enough to cover the requirements and controls needed for CSRM implementation success as prescribed by the CSRM standards/frameworks; clear in defining CSRM objectives and the responsibilities of the parties involved; communicated to the employees and stakeholders and regularly reviewed to ensure it is significant to the current needs.
Corporate governance	To confirm how corporate governance is a critical component to CSRM implementation.
Awareness	Confirms the importance of awareness programmes in developing the competency of the employees and stakeholders.
Training	Validates the impact of competency development of employees on CSRM implementation success.
IT competence	To confirm the capability to deploy and utilise technology to enhance CSRM implementation success.
System quality	To confirm if the technology's availability and reliability for performing risk management tasks are critical to CSRM implementation success.
Security audit	To the effect of monitoring, measuring and evaluating the compliance with CSRM processes, controls, and activities to ensure the effectiveness of CSRM implementation.

Appendix C: Interview Pilot Feedback

Interview Questions Pilot Feedback Form

The pilot exercise aims to ensure the quality, relevance, and ease of using the interview questions. Your feedback is, therefore, essential. Kindly review the interview questions and answer the questions below.

QUESTIONS	ANSWERS YES	NO
Do you understand the objective of the interview?		
Is the wording of the interview clear?		
Do any of the questions require you to think too long or hard before responding? If so, which one(s)?		
Do any of the questions produce embarrassment, irritation, or confusion? If so, which one(s)?		
Do any of the questions generate response bias? If so, which one(s)?		
Is the interview too long?		
Do the interview questions make use of appropriate sections?		

Provide any recommendations on how to improve the interview further:

……
……

Table C1: Pilot Interview Feedback and Actions

Feedback	Actions
Respondents might be discouraged because of the lengthy interview.	Questions reworded to avoid repetition and make more sense.
More appropriate success factors groupings should be added.	The suggested grouping added as elements under existing groups. For example, adopting a standard or framework is already captured as risk management and reframed at interview.
It may be difficult for people with little knowledge or experiences to provide the necessary responses.	Although the interview targeted experts with relevant experience in the study area, the interviewer resolved to tailor the interview to the interviewer's expertise area.

Table C2: Modified Interview Questions

Interview Questions before Modification	Modified Interview Questions
What is your job function that is related to CSRM?	What is your job function that is related to CSRM? How many years of experience on the job?
How many years of experience do you have on the job?	
Do you think your organisation's CSRM is a strategic goal and includes organisational alignment with other business goals and not only technological matter?	Describe what causes the CSRM function to be in alignment with the rest of the business?
Do you consider that the alignment of CSRM objective with strategic business goal increase your organisational cyber CSRM success?	Describe the extent to which you feel that the CSRM policies and controls are well-aligned with the rest of the business objectives, value or needs.
How would you describe the impact of top management support regarding investment/funding on CSRM success in your company?	How would you describe the impact of investment/funding planning on CSRM success in your company?
Do you think investment in CSRM creates value for the organisation?	How investment in CSRM creates value for the organisation? Please, explain.
Do you think top management support is critical for the success of CSRM implementation? Please explain	How do you think top management support is essential to the success of CSRM implementation? Please explain.
In your opinion, do you think your organisation's CSRM awareness programme has contributed to strengthening transaction security?	Explain how your organisation's CSRM awareness programme has contributed to strengthening transaction security?
How often is awareness education of cyber threats and countermeasures provided to all stakeholders or employees in your organisation?	What initiatives have your organisation taken to create CSRM implementation awareness to all stakeholders or employees in your organisation?
Do you think awareness education has reduced CSRM deficiencies in your organisation?	How has awareness education reduced CSRM deficiencies in your organisation?
In your organisation, do you have a current programme to train employees/stakeholders about policies, procedures, or countermeasures for CSRM?	In your organisation, what current programme do you have to train employees/stakeholders about policies, procedures, or countermeasures for CSRM?
Do you think the CSRM capability of all stakeholders has been beneficial to your organisation? Please explain.	How do you measure the success of a CSRM training programme on all stakeholders in your organisation?
	Please explain how you evaluate CS training effectiveness in your organisation.
Do end-users of IT systems follow sound operation processes?	How you measure end-users of IT systems follow sound CSRM operation processes? Please explain.
What are the risk management procedures/standards/or countermeasures to ensure CSRM success in your organisation?	In your organisation, what are the risk management procedures/standards/frameworks to ensure CSRM implementation success?
How effective are these procedures/standards in identifying and reducing cyber threat and attack in your organisation?	How effective are key risk management components of the standards/frameworks in identifying and reducing cyber threat and attack in your organisation?
In your organisation, what are the policies to ensure CSRM success?	What are the security policies of your organisation to ensure CSRM implementation success?
How successful is your organisation at practising CSRM policies?	On average, how many CS breaches do you experience a year at work?

Do you think the implementation of security policies in your organisation has reported fewer breaches?	How effective is implementing security policies in your organisation in reducing CS breaches in the last five years?
A literature review on prior research was used to propose a CSRM success factors framework (a recap). What is your view on the factors that have been identified as critical?	Besides what we have already discussed, what is your view on the factors identified as critical to CSRM implementation success?
Has an appropriate grouping of success factors been adopted?	What other factors impact the success of CSRM implementation in your organisation?
New factor added	Security Audit: How do you rate the effectiveness of CS audit on CSRM implementation success? Change management process:

Appendix D: List of Data Base for Used for Literature Review

Table D1: List of Data Base for Literature Review

Serial No	Name of Database	Serial No	Name of Database
1	Academic Search Complete	7	Electronic Thesis Online (ETHOS)
2	Science Direct	8	Open Access Thesis &Dissertation
3	Business Source Complete	9	Emerald Management E-Journals
4	ProQuest	10	Scopus
5	EBSCOhost	11	Sage Journal Online
6	Google Scholar	12	Decision Science

Appendix E: Summary of Previous Research related to CSRM in Nigeria

Research Topic	Reference	Methodology
Corporate governance, corporate strategy, and corporate performance: Evidence from the financial institutions listed on the Nigerian Stock Exchange	Effiok, Effiong and Usoro (2012)	Survey
Security challenges in Nigeria and the implications for business activities and sustainable development	Achumba, Ighomereho and Akpor-Robaro (2013)	Literature review
Challenges militating against the adoption of online shopping in the retail industry in Nigeria	Aminu (2013)	Literature review
Approach to cybersecurity issues in Nigeria: challenges and solution	Frank and Odunayo (2013)	Literature review
Critical Success Factors for Preventing e-Banking Fraud	Usman and Shah (2013)	Mixed method
A Socio-Technological Analysis of Cybercrime and Cyber Security in Nigeria	Olayemi (2014)	Descriptive and survey method
Risk Management Strategies in Financial Institutions in Nigeria: The Experience of Commercial Banks	Dugguh and Diggi 2015	Literature review
National Cyber Security Policy and Strategy of Nigeria: A Qualitative Analysis	Osho (2015)	Case study
Evaluating Factors of Security Policy on Information Security Effectiveness in Developing Nations: A Case of Nigeria	Okolo (2016)	Survey
Information security management needs a more holistic approach: A literature review	Soomro, Shah and Ahmed (2016)	Literature review
Cybersecurity Challenges in Nigeria: The Way Forward	Oforji, Udensi and Ibegbu (2017)	Literature review
Cyber Security Issues in Nigeria and Challenges	Makeri (2017)	Literature review
Nigerian princes to kings of malware: the next evolution in Nigerian cybercrime	Hinchliffe (2017)	Advanced Analytics
Security risk analysis and management in banking company: A Case Study of a Selected Commercial Bank in Nigeria	Gana, Shafi'i and Ojeniyi (2019)	Questionnaire
Online shopping and customers' satisfaction in Lagos state, Nigeria	Olasanmi (2019)	Questionnaire
Internet banking in Nigeria: Cybersecurity breaches, practices, and capability	Wang, Nnaji and Jung (2020)	Survey
The Evolution and Legislative Response to Nigerian Cybercrime	McCurdy (2020)	Survey
Tailored Information Security Strategies for Financial Services Companies in Nigeria	Alawonde (2020)	Qualitative Case Study

Appendix F: Informed Consent Form

Participant No.

INFORMED CONSENT FORM:
Evaluation of success factors for cybersecurity risk management in large organisations in Nigeria

You are invited to take part in this research study for the purpose of collecting data on the evaluation of success factors for cybersecurity risk management (CSRM) in the large organisations in Nigeria.

Before you decide to take part, you must **read the accompanying Participant Information Sheet.**

Please do not hesitate to ask questions if anything is unclear or if you would like more information about any aspect of this research. It is important that you feel able to take the necessary time to decide whether or not you wish to take part.

If you are happy to participate, please confirm your consent by circling YES against each of the below statements and then signing and dating the form as participant.

1	**I confirm that I have read and understood the Participant Information Sheet for the above study and have had the opportunity to ask questions**	**YES**	**NO**
2	**I understand my participation is voluntary and that I am free to withdraw my data, without giving a reason, by contacting the lead researcher and the Research Support Office at any time until the date specified in the Participant Information Sheet**	**YES**	**NO**
3	**I have noted down my participant number (top left of this Consent Form) which may be required by the lead researcher if I wish to withdraw from the study**	**YES**	**NO**
4	**I understand that all the information I provide will be held securely and treated confidentially**	**YES**	**NO**
5	**I am happy for the information I provide to be used (anonymously) in academic papers and other formal research outputs**	**YES**	**NO**
6	**I am happy for the interview to be audio recorded**	**YES**	**NO**
7	**I agree to take part in the above study**	**YES**	**NO**

Thank you for your participation in this study. Your help is very much appreciated.

Participant's Name	**Date**	**Signature**
Researcher	**Date**	**Signature**
Olukemi	**Olaniran**	

Consent form

Coventry University